

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 4 月 2 1 日
Date of Application:

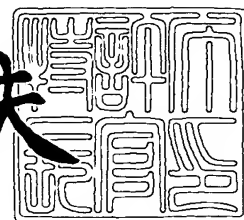
出 願 番 号 特 願 2 0 0 3 - 1 1 5 1 8 3
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 1 1 5 1 8 3]

出 願 人 株式会社日立製作所
Applicant(s):

2 0 0 3 年 7 月 3 0 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願
【整理番号】 K02014511A
【あて先】 特許庁長官殿
【国際特許分類】 G06F 13/38 340

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1099 番地 株式会社日立製作所システム開発研究所内

【氏名】 円光 豊

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区戸塚町 5030 番地 株式会社日立製作所ソフトウェア事業部内

【氏名】 藤井 直大

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書**【発明の名称】 ファイル移送装置****【特許請求の範囲】****【請求項 1】**

第一のネットワークと、前記第一のネットワークに接続される第一の計算機と、前記第一のネットワークに接続される第二のネットワークと、前記第二のネットワークに接続される第二の計算機と第三の計算機とから構成される情報処理システムにおいて、

前記第一の計算機は、前記第一のネットワークと接続するための通信インタフェースと、データを格納するディスク装置と、前記ディスク装置とデータの送受信を行うためのディスクインタフェースと、前記第一の計算機を制御するCPUと、データと前記CPUを動作させるためのプログラムを格納するメモリを備え、

前記プログラムは、前記第三の計算機からの前記ディスク装置に格納されるファイルへのアクセス状況を記録する部分と、前記アクセス状況に応じて前記ファイルを前記第二の計算機への移送候補とする部分と、前記第二の計算機へ前記ファイルの移送の受け入れの可否を問い合わせる移送許可パケットを送信する部分と、前記移送許可パケットに対する応答パケットを前記第二の計算機から受信する部分と、前記第二の計算機に前記ファイルを移送する部分を備える、情報処理システム。

【請求項 2】

前記メモリは、前記第三の計算機がアクセスするファイルのパスを、前記第三の計算機のアクセス状況を表す情報と対応付けて格納し、

前記プログラムは、前記アクセス状況を表す情報が所定の条件を満たした場合に、当該情報に対応するファイルを移送候補とする部分を備える、請求項 1 記載の情報処理システム。

【請求項 3】

前記プログラムは、前記ファイルを前記第二の計算機に移送したことを示す移送通知パケットを、前記第二のネットワークへ送信する部分を備える、請求項 2

記載の情報処理システム。

【請求項 4】

前記第三の計算機は、データとプログラムを格納するメモリを備え、

当該プログラムは、前記移送通知パケットを受信する部分と、当該パケットに応じて前記第二の計算機に対して前記ファイルのアクセスを行う部分を備える、請求項 3 記載の情報処理システム。

【請求項 5】

前記第一のネットワークは、更に第三のネットワークに接続され、

前記プログラムは、前記第二のネットワークにファイルを送送すべき計算機が存在しなかった場合、前記移送先検索パケットを前記第三のネットワークに送信する部分を備える、請求項 1 記載の情報処理システム。

【請求項 6】

第一のネットワークに接続される第一の計算機が有するファイルをアクセスし、前記第一のネットワークと通信できる第二のネットワークに接続される第二の計算機であって、

前記第二の計算機は、前記第二のネットワークと接続するためのインタフェースと、前記第二の計算機を制御する CPU と、データと前記 CPU を動作させるためのプログラムを格納するメモリを備え、

前記第一の計算機から前記ファイルを送送した先である第三の計算機へのパス名を前記インタフェースから受信した後は、前記パス名を用いて、前記インタフェースから前記ファイルへアクセスする、第二の計算機。

【請求項 7】

前記第三の計算機は、前記第二のネットワークに接続される、請求項 6 記載の第二の計算機。

【請求項 8】

前記メモリは、前記第一の計算機へのパス名と、前記第三の計算機へのパス名を対応付けて格納しており、

前記 CPU は、前記メモリを参照して、前記第三の計算機への前記パス名を用いて、前記インタフェースから前記ファイルへアクセスする、請求項 6 記載の第

二の計算機。

【請求項 9】

第二の計算機と第三の計算機が属する第二のネットワークと通信できる第一のネットワークに接続され、前記第三の計算機からファイルをアクセスされる第一の計算機であって、

前記第一の計算機は、前記第一のネットワークと接続するための通信インタフェースと、前記第一の計算機の制御を行うCPUと、データを格納するディスク装置と、前記ディスク装置にデータの送受信を行うためのディスクインタフェースと、データと前記CPUを動作させるためのプログラムを格納するメモリを備え

、
前記プログラムは、前記第三の計算機からの前記ディスク装置に格納されるファイルへのアクセス状況を記録する部分と、前記アクセス状況に応じて前記ファイルを前記第二の計算機への移送候補とする部分と、前記第二の計算機へ前記ファイルの移送の受け入れの可否を問い合わせる移送許可パケットを送信する部分と、前記移送許可パケットに対する応答パケットを前記第二の計算機から受信する部分と、前記第二の計算機に前記ファイルを移送する部分を備える、第一の計算機。

【請求項 10】

第一のネットワークに接続される第一の計算機からデータを受信し、前記第一のネットワークと通信できる第二のネットワークに接続される第二の計算機であって、

前記第二の計算機は、前記第二のネットワークと接続するための通信インタフェースと、前記第二の計算機の制御を行うCPUと、データを格納するディスク装置と、前記ディスク装置にデータの送受信を行うためのディスクインタフェースと、データと前記CPUを動作させるためのプログラムを格納するメモリを備え

、
前記プログラムは、前記第一の計算機からファイルの移送の受け入れに関する移送許可パケットを受信する部分と、前記移送許可パケットに対する応答パケットを作成する部分と、前記第一の計算機に前記移送許可パケットを送信する部分

を備える、第二の計算機。

【請求項 1 1】

第一のネットワークに接続される第一の計算機が有するファイルをアクセスし、前記第一のネットワークと通信できる第二のネットワークに接続される第二の計算機が有するメモリに格納されるプログラムであって、

前記プログラムは、前記第一の計算機から前記ファイルを送信した先である第三の計算機へのパス名を前記第二のネットワークと接続するためのインタフェースから受信した後は、前記パス名を用いて、前記インタフェースから前記ファイルへアクセスする部分を備える、プログラム。

【請求項 1 2】

第二の計算機と第三の計算機が属する第二のネットワークと通信できる第一のネットワークに接続され、前記第三の計算機からファイルをアクセスされる第一の計算機が有するメモリに格納されるプログラムであって、

前記プログラムは、前記第三の計算機からの前記第一の計算機が有するファイルへのアクセス状況を記録する部分と、前記アクセス状況に応じて前記ファイルを前記第二の計算機への移送候補とする部分と、前記第二の計算機へ前記ファイルの移送の受け入れの可否を問い合わせる移送許可パケットを送信する部分と、前記移送許可パケットに対する応答パケットを前記第二の計算機から受信する部分と、前記第二の計算機に前記ファイルを送信する部分を備える、プログラム。

【請求項 1 3】

第一のネットワークに接続される第一の計算機からデータを受信し、前記第一のネットワークと通信できる第二のネットワークに接続される第二の計算機が有するメモリに格納されるプログラムであって、

前記プログラムは、前記第一の計算機からファイルの移送の受け入れに関する移送許可パケットを受信する部分と、前記移送許可パケットに対する応答パケットを作成する部分と、前記第一の計算機に前記移送許可パケットを送信する部分を備える、プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークを介して複数の計算機（コンピュータ）が接続されたシステム（以下「ネットワークシステム」）において、あるコンピュータがネットワークを介して他のコンピュータに接続された記憶装置内のデータにアクセスする技術に関する。

【0 0 0 2】**【従来の技術】**

従来のネットワークシステムにおいて、他のコンピュータの記憶装置内のファイルに対してアクセス（読み出し(read)および書き込み(write))を要求するコンピュータを、クライアントコンピュータ（以下、単にクライアント）と呼び、クライアントからの要求に応じて自ディスク装置内のファイルをアクセスし、その結果（readデータや、正常にwriteが行われたかどうかなど）を応答するコンピュータをファイルサーバコンピュータ（以下、単にファイルサーバもしくはサーバ）と呼ぶ。

【0 0 0 3】

クライアントがネットワークを介してファイルサーバが管理するファイルにアクセスする技術として、N F S（Network File System）がある。以下、他のコンピュータが管理するファイルの読み出し又は書き込み（以下まとめて「アクセス」）を要求するコンピュータをクライアントと称する。また、クライアントからの要求に応じて、記憶装置に格納されたファイルをアクセスし、その結果（読み出したデータ、データの書き込みの完了報告等）をクライアントに応答するコンピュータをファイルサーバ又はサーバと称する。更に、ファイルとは、ユーザやコンピュータで実行されるアプリケーションプログラムが使用するデータの纏まりを指す。

【0 0 0 4】

N F Sでは、クライアントはサーバに対してR P C（Remote Procedure Call：遠隔手続き呼び出し）要求メッセージパケットを送信してアクセスを要求する。一方、サーバは、R P C応答メッセージパケットを返送してクライアントからの要求に応答する。

【 0 0 0 5 】

N F S のプロトコル設計は基本的にステートレス（サーバ・クライアント内に状態を保持しない）の方針に基づいているので、クライアントは、サーバから読み出したファイルをクライアントが有する記憶装置に一時的に保存（以下「キャッシュ」）しない。このため、クライアントが、サーバが管理するファイルをアクセスする場合には、かならずファイルサーバとの通信が発生する。

【 0 0 0 6 】

一方、ファイルサーバが管理するファイルをクライアント自身又はクライアント付近のサーバにキャッシュする技術として、分散ファイルシステム（D F S : Distributed File System）及びプロキシ（proxy : 代理）サーバがある。

【 0 0 0 7 】

D F S では、クライアントが、サーバから読み出したファイルのデータを自身の記憶装置にキャッシュする。

【 0 0 0 8 】

また、プロキシサーバは、クライアントとサーバの間（多くはクライアントと同一のネットワーク上）に設置される。クライアントはサーバへファイルのアクセスを要求する際に、プロキシサーバへアクセス要求を送信する。プロキシサーバはクライアントに成り代わってサーバからファイルを読み出し、そのファイルをクライアントへ送信する。この際、プロキシサーバは取得したファイルをプロキシサーバ内にキャッシュする。

【 0 0 0 9 】

これ以降、クライアントから再び同一ファイルのアクセス要求がプロキシサーバへ送信された場合、プロキシサーバはサーバへアクセスすることなく、プロキシサーバ内にキャッシュされたファイルをクライアントに送信する。

【 0 0 1 0 】

更に、主となるファイルサーバと副となるファイルサーバを備え、主ファイルサーバの記憶容量が不足したとき、主ファイルサーバのファイルを副ファイルサーバへ移動し、移動されたファイルに対してクライアントからアクセス要求があった場合には、主ファイルサーバが副ファイルサーバからファイルを転送しても

らうシステムが特許文献1に開示されている。

【0011】

【特許文献1】

特開平6-243074号公報

【0012】

【発明が解決しようとする課題】

NFSでは、クライアントがサーバのファイルをキャッシュしないため、クライアントが、サーバが管理するファイルへアクセスする時には、常にクライアント・サーバ間で要求パケットおよび応答パケットが往復する。このため、遠隔地にあるファイルサーバが管理するファイルをクライアントがアクセスする場合、サーバからのパケットがクライアントに到着するまでの遅延時間（レイテンシ）が増大し、クライアントのユーザに対するレスポンス性能が低下する。

【0013】

一方、DFS又はプロキシサーバのように、クライアント又はその近隣サーバにファイルをキャッシュすれば、パケット到着までのレイテンシの増加を抑えることができる。しかし、この「キャッシュ方式」には、以下の問題がある。

【0014】

「キャッシュ方式」では、サーバ内にあるファイル（元ファイル）に加え、元ファイルの複製がクライアント等に複数個作成されるので、両者の同期を取る、即ち、データの内容を一致させる処理（「一貫性制御処理」）が必要となる。特に元ファイルと複製とが保存されているコンピュータとの間の距離が長いほど本処理の実行に時間がかかる。更に、ファイルが頻繁にクライアントによって更新される場合は、頻繁に本処理を行う必要があり、「キャッシュ方式」を導入したことによるレイテンシの増加抑制の効果が減少してしまう。

【0015】

また、プロキシサーバでは、上述の一貫性制御は行われたい。したがって、最新のファイルを得たい場合には、クライアントは、再度プロキシサーバにファイルのアクセス要求を指示しなければならず、レイテンシの増大は抑制できない。

【0016】

一方、特許文献1に記載された「移送 (migration) 方式」では、一貫性制御が不要である。しかし、ファイルの格納場所が移送前後で変化するので、移送されたファイルに対するクライアントのアクセス性能が移送元よりも移送先の方が悪ければ、ネットワークシステムの性能は低下してしまう。特に、特許文献1はファイルサーバの容量不足を解消することを目的としており、アクセス性能を向上させることは考慮されていない。したがって、特許文献1では、クライアントから主ファイルサーバまでの距離よりも副ファイルサーバまでの距離のほうが遠くなって、レイテンシが増大する可能性について考慮されていない。

【0017】

特に、複数のクライアントから頻繁にアクセスされるファイルがどのファイルサーバに移送されるべきか否かは、そのファイルをアクセスする複数のクライアントがネットワークにどのように分布しているかの情報に基づいて行われることが重要であるが、従来技術では、この点について全く考慮されていない。

【0018】

本発明の目的は、クライアントが遠隔地にあるファイルサーバが管理するファイルへアクセスする際に、ファイルの一貫性を保ちつつ一貫性制御のオーバヘッドをなくし、さらに、ネットワークのトラフィックを削減することである。

【0019】

【課題を解決するための手段】

上記課題を解決するために、第一のサーバが、自ディスク装置内のファイルに対するアクセスを行うクライアントが属するネットワークの位置情報を検査し、ファイルの移送先となるサーバの候補を決定する。そして、アクセスを行うクライアントのネットワーク、もしくは、その周辺のネットワーク上の、不特定多数のサーバへ、ファイルを移送するサーバを調べるための移送先検索パケットを送信する。移送先検索パケットを受信した第二のサーバは、ファイルの移送の受け入れに関する移送許可パケットを第一のサーバに対して送信する。第一のサーバは、移送許可パケットの内容を検査し、第二のサーバがファイルを移送するのに適していることが分かれば、第二のサーバに対してファイルを移送する。

【0020】

更に、第一のサーバは、ファイルを送送したことを示す移送通知パケットを、アクセスを行うクライアントのネットワーク、もしくは、その周辺のネットワークに送信するため、クライアントは、移送したファイルに対するアクセスを、第二のサーバに対して行う。

【 0 0 2 1 】

【発明の実施の形態】

図 1 は、本発明を適用したネットワークシステムの一実施形態を示す図である。本ネットワークシステムは、3 台のファイルサーバ105、具体的には、ファイルサーバ105 A、105 B 及び105 C、並びに 3 台のクライアント103、具体的には、クライアント103 A、103 B 及び103 C を有する。ファイルサーバ105 A、ファイルサーバ105 B、クライアント103 A 及びクライアント103 B は、通信線（ここではローカルエリアネットワーク。以下「LAN」）101 A（以下「LAN1」）を介して相互に接続されている。ファイルサーバ105 C 及びクライアント103 C は、LAN101 B（以下「LAN2」）を介して相互に接続されている。

【 0 0 2 2 】

また、本例では、LAN1 及び LAN2 は、インターネットや WAN といった広域ネットワーク 104 により相互に接続されている。更に、LAN1 にはネットワークマスク 100 . 0 . 0 . 0 / 24 が、LAN2 には、ネットワークマスク 200 . 0 . 0 . 0 / 24 が与えられている。尚、本実施形態では通信線 101 として LAN を一例としてあげたが、他の通信線を用いても構わない。

【 0 0 2 3 】

また、本明細書では、インターネットプロトコルバージョン 4（以下 IPv4）技術で用いられるアドレス表記をネットワークマスク等の表記に用いる。ここで、本実施形態のネットワークに接続されるコンピュータ等の機器には、それぞれ固有の 32bit の IP アドレス（例えば「100 . 0 . 0 . 1」）が割り振られる。また、ネットワークマスクの表記、例えば LAN1 に割り振られたネットワークマスク「100 . 0 . 0 . 0 / 24」の表記は、LAN1 に接続されたコンピュータに、いずれも上位 24bit 共通の IP アドレスが割り振られている、すなわち、LAN1 に接続されるコンピュータに、「100 . 0 . 0 . 0」～「100 . 0 . 0 . 255」の範囲の IP アドレスが割り振られることを示している。

したがって、LAN1に接続される機器は、LAN1に割り振られたネットワークマスクによって一つのグループ（以下「ネットワークグループ」）として識別されることになる。

【0 0 2 4】

各ファイルサーバ105は計算機であり、CPU117、メモリ101、ネットワークインターフェイス117、ディスク I O インターフェイス118、及びディスク装置119を有する。CPU117、メモリ101、ネットワークインターフェイス117及びディスク I O インターフェイス118は、接続線を介して相互に接続されている。また、ディスク装置119は、ディスク I O インターフェイス118を介してCPU117等と接続されている。更に、ファイルサーバ105は、ネットワークインターフェイス117を介してLAN101と接続される。

【0 0 2 5】

尚、ファイルサーバ105自身はディスク装置119を有さない構成としても良い。この場合、ファイルサーバ105はディスク I O インターフェイス118の代わりにネットワークインターフェイスを有し、ファイルサーバ105は、このインターフェイス及びネットワークを介して別筐体の記憶装置システムに接続されている構成とする。ここで使用されるインターフェイス及びネットワークには、例えば、ファイバチャネルプロトコルが使用される。あるいは、ファイルサーバ105は、ファイルシステム機能に特化したネットワークアタッチドストレージ（NAS）でも良い。

【0 0 2 6】

更に、ファイルサーバ105は、ディスク装置119を有し、かつ別筐体の記憶装置システムに接続するためのネットワークインターフェイスを有する構成としても良い。

【0 0 2 7】

ここで、記憶装置システムとは、記憶媒体及び制御部を有する記憶装置である。記憶媒体には、磁気ディスク又は光ディスク等が使用される。また、記憶装置システムには、冗長構成を有するディスクアレイも含まれる。尚、ファイルサーバ105が有するディスク装置119は、単体のハードディスクドライブでも、ディス

クアレイ、DVD等でも良い。

【 0 0 2 8 】

メモリ101には、ファイルシステムプログラム120、ノード・パス名変換テーブル121及びアクセス統計テーブル122が格納される。図では、テーブルの情報やプログラムは丸で囲んで示している。これらのプログラムやテーブルは、電源オフ時にはファイルサーバ105が有する不揮発性記憶媒体（ディスク装置119やROMなど）に格納されている。ファイルサーバ105は、これらのテーブルやプログラムを使用する際に、不揮発性記憶媒体からメモリ101にこれらのプログラム等を読み出す。ファイルシステムプログラム120等のプログラムは、フロッピー（登録商標）ディスクやDVDの記憶媒体、ネットワーク等の通信回線あるいは無線通信等を介してファイルサーバ105のディスク装置119又はメモリ101にインストールされる。

【 0 0 2 9 】

CPU116は、ファイルシステムプログラム120を実行し、LAN101等に接続された他のファイルサーバ105等とのパケット通信、ディスク装置119へのアクセス、メモリ101内のデータの更新、等を行う。

【 0 0 3 0 】

また、各クライアント103もファイルサーバ同様に、CPU116、メモリ111、ネットワークインターフェイス117を有する計算機である。尚、本実施形態では、クライアント103はディスク装置119の代わりにROM装置110を有する。クライアント103をファイルサーバ105と同じ構成とすることもできる。クライアント103は、ネットワークインターフェイス116を介してLAN101と接続される。

【 0 0 3 1 】

クライアント103のメモリ111には、アプリケーションプログラム113、ファイルシステムプログラム114及びノード・パス名変換テーブル115が格納される。これらのプログラム等は、電源オフ時には、ROM装置110に格納されている。

【 0 0 3 2 】

クライアント103のCPU116は、ファイルシステムプログラム114を実行し、LAN101を介してファイルサーバ105のディスク装置119に格納されているファイルにア

クセスする。また、クライアント103のCPU116は、アプリケーションプログラム113を実行して、クライアントを使用する人が所望するサービスを提供する。

【0033】

本実施形態のファイルシステムプログラム114、120によって実現されるファイルシステムは、UNIX（登録商標）その他の一般的なOSに採用されているように、論理的な木構造の元にファイルを管理する階層型のファイルシステムである。具体的には、ルート・ディレクトリを根とし、ディレクトリの下にファイルもしくはディレクトリを配するデータ構造が用いられる。本実施形態では、ファイルシステムで管理されるファイルを、「/doc/misc/readme.txt」のように、ディレクトリ名の接続とファイル名を区切り文字("/")で区切った文字列（以下、「ファイルのパス名」）により表す。

【0034】

図2は、本実施形態のクライアント103とサーバ105間でやり取りされるアクセス要求および応答パケットの例を示す図である。LAN101での通信は、所定の通信プロトコルに基づくパケットによるデータ送受信でおこなわれる。クライアント103は、図2のA及びBに示す読み出し（以下「read」）及び書き込み（以下「write」）要求パケットをファイルサーバ105へ送信する。ファイルサーバ105は、図2のC及びDに示すread/write返答パケットをLAN101を介してクライアント103へ返信する。

【0035】

図2Aは、クライアントA（送り元フィールド値に100.0.0.1のクライアントAのIPアドレスが格納されている）がファイルサーバC（宛先フィールドが200.0.0.101）に対して、ファイル"/doc/misc/sample.log"（要求パス名）の先頭から4096byte目（オフセット）から1024byte（サイズ）をread要求（要求種別）するパケットである。

【0036】

図2Bは、クライアントA（送り元）がファイルサーバC（宛先）に対して、ファイル"/doc/misc/sample.log"（要求パス名）の先頭から4096byte目（オフセット）から1024byte（サイズ）にデータ本体（データフィールドに格納）をwrite

e要求（要求種別）するパケットである。

【0 0 3 7】

図 2 Cは、サーバC（送り元）がクライアントA（宛先）に、read応答（要求種別）を返すパケットである。ファイル” /doc/misc/sample.log”（要求パス名）の先頭から4096byte目（オフセット）から1024byte（サイズ）をデータフィールドに格納して返答している。

【0 0 3 8】

図 2 Dは、サーバC（送り元）がクライアントA（宛先）に、write応答（要求種別）を返すパケットである。ファイル” /doc/misc/sample.log”（要求パス名）の先頭から4096byte目（オフセット）から1024byte（サイズ）が正常に書き込まれたことを返答している。

【0 0 3 9】

各ファイルサーバ105のCPU116は、ファイルシステムプログラム120を実行することで、クライアント103からのアクセスを監視し、その結果をアクセス統計テーブル122に格納する。

【0 0 4 0】

図 3 は、アクセス統計テーブル122の例を示す図である。アクセス統計テーブル122には、クライアント103からアクセスされたファイルのパス名を登録するエントリ601、要求元となるクライアント103が所属するネットワークグループに共通するネットワークマスクを登録するエントリ602、ネットワークまでの距離（ただし、主にホップ数（中間ルータの数）や、遅延時間、通信料金、信頼性などにより算出される距離であり、物理的な距離を意味しない。）が登録されるエントリ603、そのネットワークグループに属するクライアント103からのアクセス回数を登録するエントリ604及びそのネットワークグループに属するクライアント103から最初にアクセスがあった時刻を記録するエントリ605を有する。また、本テーブル122には、ファイル毎にこれらの情報が登録される。

【0 0 4 1】

ここで、本発明の動作の概要を簡単に説明すると、ファイルサーバがアクセス統計テーブルの内容を確認し、移送対象となるファイルを探し出し、次に移送先

となるファイルサーバを決定し、ファイルの格納位置情報を変更し、その後に、ファイルの実体を移行する。以下、動作の手順を追って説明する。

【 0 0 4 2 】

図 4 は、サーバ105が、アクセス統計テーブル122を更新する際の処理手順の例を示した図である。尚、本処理手順は、ファイルサーバ105が、クライアント103からのファイルアクセス要求を受信したときに実行される。

【 0 0 4 3 】

クライアント103からファイルアクセス要求を受信したサーバ105は（ステップ701）、まず、自身のメモリ101内のアクセス統計テーブル122に、アクセス要求を受けたファイルのエントリが既に存在するかどうかを調べる（ステップ702）。

【 0 0 4 4 】

アクセス統計テーブル122にアクセス要求を受けたファイルのエントリが存在しなければ、サーバ105は、アクセス統計テーブル122に新たにエントリを作成し、エントリ601に、アクセス要求を受けたファイルのパス名を登録する（ステップ703）。

【 0 0 4 5 】

アクセス統計テーブル122にアクセス要求を受けたファイルのエントリが既に存在する場合、サーバ105は、存在するファイルに対応するエントリ602に登録されたネットワークマスクに対応するネットワーク101が、ファイルアクセスを要求したクライアント103が属するネットワークグループのネットワーク101と一致するか検査する。具体的には、アクセス要求パケットに含まれる宛先（サーバ）エントリに登録されたアドレスの上位24Bit（ただし、24は、マスクビット長の例。）とエントリ602に登録されたネットワークマスクの値とを比較する（ステップ704）。

【 0 0 4 6 】

アクセス要求元であるクライアント103が属するネットワークグループに対応するネットワーク101と登録されたネットワークマスクに対応するネットワーク101とが異なる場合及びステップ703にて新たにファイルのエントリを作成した場合、サーバ105は、アクセス要求の対象となるファイルに対応するエントリ602に

、クライアント103が属するネットワークグループのネットワークマスクを登録する。また、サーバ105は、アクセス要求の対象となるファイルに対応するエントリ603に、クライアント103が属するネットワークグループとサーバ105が属するネットワークグループとの間の距離（ここではクライアント103が属するネットワークグループとサーバ105が属するネットワークグループとの間に存在する、ネットワークを仲介する中間ルータ数）を登録する。尚、インターネットの場合、各装置間の距離（ホップ数）はICMPパケット等を用いて算出することができる。

【 0 0 4 7 】

さらに、サーバ105は、アクセス対象のファイルに対応するエントリ604に値「1」を設定し、エントリ605に、現在時刻（ここでは、テーブルに値を設定するときの時刻）を設定する(705)。

【 0 0 4 8 】

ステップ704でアクセス要求元のクライアント103が属するネットワークグループがアクセス統計テーブル122に登録されたネットワークグループと同一であると判断した場合、サーバ105は、アクセス要求のあったファイルに対応するエントリ604に登録された値を1増分（インクリメント）する(ステップ706)。ステップ705又はステップ706の処理を実行したサーバ105は、アクセス統計テーブルの更新処理を終了する。

【 0 0 4 9 】

現在時刻が「2002/9/1 10:00:00」から0.300秒後の場合、図3で例示したアクセス統計テーブル122の1行目は、ファイルサーバ105のファイル"/doc/misc/record.out"に対して、LAN1(100.0.0.0/24)のネットワークグループに属するクライアント103(サーバ105との間の距離は5)から、0.300秒間（「現在時刻－アクセス開始時刻」にて算出）に連続して120回のアクセスが発生したことを示している。

【 0 0 5 0 】

ここで、仮にクライアント103Cがファイルサーバ105Cのファイル"/doc/misc/record.out"に対してread要求を発行すると、クライアント103Cの属するネット

ワークグループ（ここではLAN2）は、その前に登録されていたネットワークグループ（ここでは、LAN1）とは異なるので、図3の第一行目の内容は、図4で示した処理により、”/doc/misc/record.out”，”200.0.0.0/24”，”1”，”1”，”現在時刻”と書き換えられる。

【0051】

各ファイルサーバ105は、一定時間毎にアクセス統計テーブル122の内容を検査し、ファイルサーバ105が管理するファイルに対して、特定のネットワークグループに属する任意のクライアント103からのアクセス（以下「ネットワークグループからのアクセス」と称する）が集中（詳細は後述）しているかどうかを確認する。もしそのようなファイルが見つかったときは、ファイルサーバ105は、そのファイルを移送すべきファイルの候補として選定する。

【0052】

図5は、サーバ105がアクセス統計テーブル122の内容を確認して移送すべきファイルの候補を選択するまでの処理手順の例を示すフローチャートである。本処理は、ファイルサーバ105が、ファイルシステムプログラム120を実行することによって一定時間毎に実行される。

【0053】

ファイルシステムプログラム120を実行するファイルサーバ105Cは（ステップ801）、アクセス統計テーブル122の内容を確認し、予め定められた条件を満たすファイルが存在するかどうかを確認する。尚、本実施形態では、移送候補となるファイルとして、クライアント103が属するネットワークグループとファイルサーバ105が属するネットワークグループとの間の距離が2以上、あるネットワークグループからのアクセス回数が10回以上、かつ、アクセス開始時刻から現在時刻まで1時間以上経過している（その間、他のネットワークグループからのアクセスはない）ファイルが検出されるよう、条件が設定される（ステップ802）。

（ただしこれらの閾値はファイルシステムプログラムにあらかじめ設定するほか、ユーザにより再設定する。）

条件を満たすファイルがある場合、サーバ105Cは、そのファイルを移送候補として選択する。例えば、現在時刻が仮に2002/9/2 11:00:05（2002年9月2日 11時

00分05秒) ならば、図3のアクセス統計テーブル122の例では、ファイル”/doc/misc/record.out”が条件に適合している。このため、ファイル”/doc/misc/record.out”が移送候補として選定される(ステップ803)。

【0054】

移送候補となるファイルを選定したら、ファイルサーバ105Cは、次に、選定されたファイルを集中的にアクセスしているネットワークグループに属するファイルサーバ105へ、選定されたファイルを移送しようと試みる。上記の例では、ファイルサーバ105Cは、選定されたファイル”/doc/misc/record.out”を、アクセスを行っているネットワークグループ(ここではLAN1)に属するファイルサーバ105Aまたは105BをLAN1から検索する。具体的には、ファイルサーバ105Cは、移送先検索パケットをLAN1に接続されている機器に対してブロードキャストする。ここで、ブロードキャストとは、指定したネットワークに属する不特定の機器(ノード)を受信先としたパケットの送信を指す(ステップ804)。

【0055】

図6は、移送先検索パケットの例を示す図である。移送先検索パケットは、移送元となるファイルサーバ105C(以下「移送元ファイルサーバ」)が、ファイルを特定のネットワークグループのいずれかのファイルサーバ105Aまたは105Bへ移送することが可能かどうか判断するために発行する。すなわち、移送先となるファイルサーバ105Aまたは105B(以下「移動先ファイルサーバ」)を検索するために発行される。

【0056】

移送先検索パケットの「宛先ネットワーク」は移送先検索パケットのブロードキャスト先ネットワークマスクを格納する。「送り元サーバ」は本パケットの発行元ノードのIPアドレスを格納する。「移送ID」は一連の移送手続きを他の移送手続きと区別するために移送元ファイルサーバが付ける識別番号である。「移送元サーバ」は移送元サーバのIPアドレスである。

【0057】

移送先検索パケットは、要求容量フィールドを有する。同フィールドには、移送元ファイルサーバが移送するファイル(以下「移送ファイル」)を格納するた

めに、移送先ファイルサーバ105Aまたは105Bに確保すべき記憶容量が設定される。具体的には、移送ファイルのサイズ（もしくはファイルサイズが拡大することを見越してそれ以上の値）が設定される。

【0058】

移送先検索パケットを受け取ったLAN1のネットワークグループに属するファイルサーバ105Aと105Bは、指定された移送ファイルを受け入れることができるかどうかを判定し、その結果を移送元ファイルサーバに送信する。

【0059】

図7は、移送先検索パケットを受信したサーバ105Aと105Bが実行する移送受け入れ判定処理のフローチャートを示す図である。本処理は、ファイルサーバ105Aと105Bがファイルシステムプログラム120を実行することによって行われる。

【0060】

移送先検索パケットを受け取ったファイルサーバ105Aと105Bは、移送許可パケットを作成する。図8は、移送許可パケットの具体例を示す図である。ファイルサーバ105Aと105Bは、移送許可パケットの管理者フィールドに、サーバを管理する管理者の管理者ID（本例では"foo"）を設定する。さらに、なりすましを防止し、管理者が本物であることを示すために、ファイルサーバ105は、暗号化された管理者署名（本例では"oekdigke"）を管理者署名フィールドに設定する（ステップ1002）。

【0061】

次に、ファイルサーバ105Aと105Bは、移送ファイルを受け入れることが可能かどうかを判定するために、自らが有するディスク装置119の空き容量を検査する。ファイルサーバ105Aと105Bは、ディスク装置119に移送先検索パケットで指定された要求容量以上の空き容量が存在する場合は、移送ファイルを受け入れることができると判断する。ディスク装置119に移送先検索パケットで指定された要求容量以上の空き容量が存在しない場合は、ファイルサーバ105A, 105Bは、移送ファイルを受け入れることができないと判断する（ステップ1003）。

【0062】

移送ファイルを受け入れることができる場合、ファイルサーバ105A, 105Bは、

作成した移送許可パケットの応答フィールドに受け入れ許可を示す数値、ここでは1を設定する。また、ファイルサーバ105A, 105Bは、移送許可パケットの許容量フィールドに、ディスク装置119の記憶容量の空き容量を示す値をセットする。さらに、ファイルサーバ105A, 105Bは、移送ファイルを受け入れるためのディレクトリ（本例では、ディレクトリ"/200.0.0.101/"）をディスク装置119に作成し、移送許可パケットの移送先パス名フィールドに作成したディレクトリのパス名を示す情報をセットする（ステップ1004）。

【0063】

移送ファイルを受け入れることができない場合、ファイルサーバ105A、105Bは、作成した移送許可パケットの応答フィールドに、転送受け入れの不可を示す値、ここでは0を設定する（ステップ1005）。

【0064】

本実施形態では、移送先ファイルサーバの候補であるLAN1のネットワークグループに属するファイルサーバ105A及び105Bが、それぞれ図8A、Bに示した移送許可パケットを移送元ファイルサーバ105Cへ返送したとする。

【0065】

ファイルサーバ105A及び105Bから移送許可パケットを受信したファイルサーバ105Cは、受信した移送許可パケットの内容を比較して、移送先ファイルサーバを決定する。

【0066】

図9は、移送元となるファイルサーバ105、ここではファイルサーバ105Cが、移送先ファイルサーバの決定する際の処理手順を示すフローチャートである。本処理は、移送許可パケットを受信したときに、ファイルサーバ105Cがファイルシステムプログラム120を実行することによって実行される。

【0067】

まず、ある移送許可パケットを受信したファイルサーバ105Cは、他の移送許可パケットの到着を一定時間待つ（ステップ1302）。もし、移送先検索パケットをブロードキャストした後、一つも移送許可パケットを受信しない場合、ファイルサーバ105Cは受け入れ先無しとみなして何もしない。また、一定時間経過後に到

着した移送許可パケットは無視される。その後、ファイルサーバ105Cは、その一定期間内に到着した移送許可パケットの中から、移送許可パケットの応答フィールドに移送許可を示す1が登録されている移送許可パケットを選択する(ステップ1303)。

【0068】

その後、ファイルサーバ105Cは、選択された移送許可パケットの中から、その管理者IDフィールドに登録された管理者IDがファイルサーバ105Cの管理者と同一の管理者IDであり、かつ管理者署名フィールドに登録されている暗号署名に基づいてその管理者IDが本物であると認証できた移送許可パケットを選択する。尚、移送許可パケットを送信したファイルサーバ105A、105Bの管理者が移送元ファイルサーバの管理者と同じでなければ、そのサーバ105は信頼できないとみなして移送先ファイルサーバとしなくても良い。ただし、管理者が異なる場合でも、あらかじめ許容される複数の管理者名が移送元ファイルサーバに登録され、移送許可パケットに登録された管理者がその複数の管理者に含まれる場合には、移送元ファイルサーバがファイルの移送を行う態様としても良い(ステップ1304、1305)。

【0069】

その後、ファイルサーバ105Cは、選択された移送許可パケットの中から、確保容量フィールドに登録された記憶容量が最大のものを選択する(ステップ1306)。その結果、ファイルサーバ105Cは、選択された移送許可パケットを発行したファイルサーバ105Aを移送先ファイルサーバとして選択する(本例では、ファイルサーバAを選択したとする)。尚、ステップ1306で条件に合致する移送許可パケットとして複数の移送許可パケットが残った場合には、ファイルサーバ105Cは、そのうちのひとつをランダムに選択する。本実施形態では、図8A、Bの移送許可パケットを受け取ったファイルサーバ105Cは、空き容量が最大のファイルサーバ105Aを移送先ファイルサーバとして選択する(ステップ1307)。

【0070】

上述した各ステップにおいて、条件に一致する移送許可パケットが見つからなかった場合は、ファイルサーバ105Cは、移送先ファイルサーバ無しとして、以

下に述べる移送先ファイルサーバの指名処理は行わない。すなわち、ファイルサーバ105Cは、ファイルの移送をおこなわない(ステップ1308)。

【0071】

移送先ファイルサーバを決定した、移送元ファイルサーバ105Cは、ファイルシステムプログラム120を実行して、ノード・パス名変換テーブル121を更新する。この更新により、移送ファイルを管理するファイルサーバ105が、移送元ファイルサーバ105Cから移送先ファイルサーバ105Aへと変更される。

【0072】

図10は、ノード・パス名変換テーブル121の例を示す図である。ノード・パス名変換テーブル121には、移送ファイルの移送元と移送先ファイルサーバに関する情報が関連付けて登録される。ファイルサーバ105は、このテーブルを検索して、ファイルが移送されているかどうか及び移送されている場合にはその移送先についての情報を取得することが出来る。

【0073】

移送先ファイルサーバを決定した移送元ファイルサーバ105Cは、ノード・パス名変換テーブル121に、決定された移送先ファイルサーバに対応する新たなエントリ(行)を追加し、移送元のノード及びパス名フィールド、移動先のノード及びパス名フィールドに値をセットする。尚、「移送ID」は一連の移送手続きを他の移送手続きと区別するために移送元ファイルサーバが付ける識別番号である。移送元ファイルサーバが移送先検索パケット内に設定する。

【0074】

移送元のノードフィールドには、自ファイルサーバ105(この場合105C)のIPアドレス(本例では200.0.0.101)がセットされる。移送元のパス名フィールドには、移送ファイルのパス(本例では"/doc/misc/record.out")がセットされる。

【0075】

移送先のノードフィールドには、選択された移送許可パケットの移送先サーバフィールドに登録された値(本例では100.0.0.101)がセットされる。移送先のパス名フィールドには、選択された移送許可パケットの移送先パス名フィールド

に登録された値（本例では"/200.0.0.101/doc/misc/record.out"）がセットされる。

【0076】

その結果、ノード・パス名変換テーブル121の新たなエントリには、"200.0.0.101"の"/doc/misc/record.out"としてファイルサーバ105Aに管理されていたファイルが、"100.0.0.101"の"/200.0.0.101/doc/misc/record.out"に移送されたことを示す情報が登録されることになる。

【0077】

ノード・パス名変換テーブル121を更新したファイルサーバ105Cは、ファイルサーバ105Aが移送先ファイルサーバとして選択され、ファイルがファイルサーバ105Aへ移送されたことをクライアント103及びファイルサーバ105へ通知するために、移送先ファイルサーバが属するネットワークグループのネットワークであるLAN1へ移送通知パケットをブロードキャストする(ステップ1309)。

【0078】

尚、移送通知パケットがブロードキャストされる時点で、実際にファイルが移送されていても、移送されていなくても良い。ファイルが移送されていない場合、そのファイルの移送は、クライアント103から移送ファイルに対するアクセス要求があったタイミングで、移送先ファイルサーバの要求に基づいて行われても良い。このようにすることによって、移送が必要なファイル（移送ファイルとして決定されても、実際にその後アクセス要求がなければ、移送する必要はない）のみ移送することができ、移送ファイルの移送によるネットワーク101の負荷の増加を最小限に抑えることができる。

【0079】

また、実際のファイルの移送を、移送通知パケットのブロードキャスト後で、アクセス要求とは無関係な任意の時点にすることもできる。例えば、ネットワーク101のトラフィックが少ない時を見計らってファイルの移送が行われても良い。一方、移送通知パケットをブロードキャストする前に、移送ファイルが実際に移送されても良い。この場合、アクセス要求があった際に行われる移送元ファイルサーバでの処理量が少なくなるというメリットがある。

【0080】

図11は、移送通知パケットの例を示す図である。同図の移送通知パケットには、移送元ファイルサーバに関する情報と移送先ファイルサーバに関する情報が含まれる。本図の移送通知パケットは、“200.0.0.101”の”/doc/misc/record.out”としてファイルサーバ105Aが管理していたファイルが、ファイルサーバ105C（“100.0.0.101”）の”/200.0.0.101/doc/misc/record.out”に移送されたことを示している。

【0081】

移送通知パケットを受信したファイルサーバ105Aおよびクライアント103Aは、移送元ファイルサーバ（ここではファイルサーバ105C）が行ったのと同様に、ノード・パス名変換テーブル115、121に新たなエントリ（行）を追加し、移送元のノード及びパス名フィールド、移送先のノード及びパス名フィールドに値をセットする。

【0082】

次に、移送ファイルをクライアント103Aがアクセスする場合の動作について説明する。

【0083】

図12は、クライアント103におけるアクセス変換処理の手順を示すフローチャートである。本処理は、クライアント103がファイルシステムプログラム114を実行することで実行される。本実施形態では、クライアント103Aが、ファイルサーバ105Cが管理するファイル（パス名”/doc/misc/record.out”）にアクセスする例を示す。ここで、クライアント103Aのアプリケーションプログラム113は、ファイルの移送の有無について関知しないため、ファイルサーバ105Cが管理するファイル”/doc/misc/record.out”を、移送の有無を問わず、そのままアクセスしようとする。

【0084】

アプリケーションプログラム113の実行によってアクセス要求パケットを作成したクライアント103Aは、作成されたアクセス要求（ここではファイルサーバ105Cが管理するファイル”/doc/misc/record.out”）に基づいてノード・パス名変

換テーブル115を参照し、アクセスしようとするファイルが同テーブル115の移送元フィールドに存在するかどうかを確認する(ステップ1602)。

【0085】

アクセス要求の対象となるファイルを有するファイルサーバ105Cがノード・パス名変換テーブル115の移送元フィールドに存在しなければ、クライアント103Aは、そのままファイルサーバ105、ここではファイルサーバ105Cへアクセス要求パケットを発行する(ステップ1604)。

【0086】

アクセス要求の対象となるファイルを有するファイルサーバ105Cがノード・パス名変換テーブル115の移送元フィールドに存在する場合、そのファイルは別のファイルサーバ105Aへ移送されているので、クライアント103Aは、アクセス要求パケットの送付先を移送先ファイルサーバへに変換してアクセス要求パケットを発行する。本実施形態では、アクセスしようとするファイル(“/doc/misc/record.out”)がテーブル115の移送元フィールドに存在するため、クライアント103Aは、ファイルへのアクセス要求の発行先を、テーブル115の移送先フィールドに記述されたファイルサーバ(IPアドレス：100.0.0.101) 105Aの「200.0.0.101/doc/misc/record.out」に変換してアクセス要求パケットを発行する。

【0087】

図13は、変換前と変換後のアクセス要求パケットの例を示す図である。クライアント103Aにおける変換により、宛先(サーバ)フィールドがノード・パス名変換テーブル115の移送先ノードフィールドに登録された値(100.0.0.101)に変換され、要求パス名フィールドがテーブル115の移送先パス名フィールドに登録された値(/200.0.0.101/doc/misc/record.out)に変換される(ステップ1603、1604)。

【0088】

次に、移送ファイルに対するアクセス要求を受けた移送先ファイルサーバ105Aの動作を説明する。

【0089】

図14は、アクセス要求を受け付けた移送先ファイルサーバ105Aの処理手順を

示すフローチャートである。

【0090】

アクセス要求パケット（本例では、図13の変換後のアクセス要求パケット）を受け付けた移送先ファイルサーバ105Aは、アクセス要求パケットの要求パス名フィールドに記されたファイル（本例では、パス名が"/200.0.0.101/doc/misc/record.out"）が既に自分のディスク装置119に格納されているかどうかを検査する（ステップ1802）。

【0091】

既にディスク装置119にファイル"/200.0.0.101/doc/misc/record.out"が存在する場合、そのファイルは移送済みなので、ファイルサーバ105Aは、そのままファイルにアクセスし、そのアクセス結果に基づいて返答パケットを生成し、クライアント103Aへ応答パケットを送信し（ステップ1807）、手続きを完了する。

【0092】

一方、ファイル"/200.0.0.101/doc/misc/record.out"がディスク装置119に格納されていない場合、ファイルサーバ105Aは、そのファイルのパス名がノード・パス名変換テーブル121の移送先フィールドに存在するかどうかを確認する（ステップ1803）。

【0093】

ノード・パス名変換テーブル121の移送先フィールドにファイルのパス名が存在しない場合、そのファイルはシステムのどのファイルサーバ105A, 105B, 105Cにも存在しないので、ファイルサーバ105Aは、クライアント103Aにファイルが存在しないことを示すエラーを送信し（ステップ1804）、手続きを完了する。

【0094】

ノード・パス名変換テーブル121の移送先フィールドにファイルのパス名が存在する場合、そのファイルはまだ移送元ファイルサーバ105Cから移送先ファイルサーバである本ファイルサーバ105Aに移送されていないことになる。そこで、ファイルサーバ105Aは、ノード・パス名変換テーブル121の移送元フィールドを参照し、ファイルのパス名に対応する移送元ファイルサーバC（200.0.0.101）及びファイルのパス名（"/doc/misc/record.out"）を取得する。更に、ファイルサー

バ105Aは、取得した移送元ファイルサーバ105Cへファイルのread要求パケットを発行する。さらに、ファイルサーバ105Aは、移送元ファイルサーバ105Cに格納されている移送ファイルを削除する要求パケットも発行する。尚、read要求パケット及び移送ファイルの削除を要求する要求パケットを受信した移送元ファイルサーバ105Cは、read要求パケットで指定されるファイルを、read要求パケットを発行したファイルサーバ105Aへ送信し、その送信したファイルをディスク装置119から削除する。尚、移送元ファイルサーバ105Cにread要求パケットで指定されるファイルが存在しない場合、移送元ファイルサーバ105Cは、read要求パケットを発行したファイルサーバ105Aにエラーを報告する(ステップ1805)。

【 0 0 9 5 】

移送元ファイルサーバからread応答パケットが返信されると、ファイルサーバ105Aは、受信したread応答パケットに含まれるファイルのデータを、自ディスク装置119に格納する。このときのファイルのパス名は、ノード・パス名変換テーブル121の移送先のパス名フィールドに格納された値 (“/200.0.0.101/doc/misc/record.out”) が用いられる(ステップ1806)。

【 0 0 9 6 】

最後に、ファイルサーバ105Aは、ディスク装置119に格納したファイル“/200.0.0.101/doc/misc/record.out”へアクセスし、クライアント103Aへ応答パケットを送信し(ステップ1807)、応答処理を完了する。

【 0 0 9 7 】

次に、移送先通知パケットを受信しなかったクライアント103 (例としてクライアント103C) が、移送済みの移送ファイル (“/doc/misc/record.out”) にアクセスする動作について説明する。

【 0 0 9 8 】

移送通知パケットは、ある条件を満たしたアクセス要求元のクライアント103が属するネットワークグループのネットワーク101へブロードキャストされるため、その他のネットワークグループ(ここでは例としてLAN2)に属するクライアント103Cには、ファイル(例として、ファイルサーバ105Cの“/doc/misc/record.out”)が移送先ファイルサーバ(例としてファイルサーバ105A)へ移送された

ことが通知されない。また、本発明が適用されないクライアントがネットワーク 101 に多数属する環境でも、ファイルは全てのクライアントから正常にアクセスできなければならない。

【 0 0 9 9 】

図 1 5 は、ファイルが移送されたことを知らないクライアント 103C がファイルサーバ 105C（この場合、ファイルサーバ 105C は移送元ファイルサーバとなる）にアクセス要求パケットを発行した時の、ファイルサーバ 105C の応答処理の手順を示すフローチャートである。

【 0 1 0 0 】

アクセス要求パケット（本例では、図 1 6 の変換前要求パケット）を受信したファイルサーバ 105C は、アクセス要求パケットの要求パス名フィールドに登録されたファイル”/doc/misc/record.out”が自ディスク装置 119 に格納されているかどうかを検査する（ステップ 1902）。

【 0 1 0 1 】

ファイル”/doc/misc/record.out”が自ディスク装置 119 に格納されている場合、ファイルサーバ 105C は、そのファイルにアクセスし、その結果に基づいて返答パケットを生成し、クライアント 103C へ応答パケットを送信し（ステップ 1903）、応答処理を完了する。

【 0 1 0 2 】

ファイル”/doc/misc/record.out”が自ディスク装置 119 に格納されていない場合、ファイルサーバ 105C は、そのファイルのパス名がノード・パス名変換テーブル 121（本例では、図 1 0 のテーブル 121 をファイルサーバ 105C が有しているとする）の移送元フィールドに存在するかどうかを確認する（ステップ 1904）。ノード・パス名変換テーブル 121 の移送元フィールドにそのファイルのパス名が存在しない場合、そのファイルはネットワークシステムのどこにも存在しないので、ファイルサーバ 105C は、クライアント 103C へファイルが存在しないことを示すエラーを送信し（ステップ 1905）、応答処理を完了する。

【 0 1 0 3 】

ノード・パス名変換テーブル 121 の移送元フィールドにファイルのパス名が存

在する場合、そのファイルは既に移送先ファイルサーバへ移送されていることになる（図 1 0 では、ファイル”/doc/misc/record.out”の移送先ファイルサーバは、200.0.0.101の”/doc/misc/record.out ”となる）。そこで、ファイルサーバ105Cは、ノード・パス名変換テーブル121において、検索されたファイルのパス名に対応する移送先フィールドを参照し、移送先ファイルサーバ（100.0.0.101）及び移送先でのファイルのパス名（”/200.0.0.101/doc/misc/record.out”）の情報を取得する。

【 0 1 0 4 】

次に、ファイルサーバ105Cは、クライアント103Cから受信したアクセス要求パケット（図 1 6 の変換前要求パケット）の宛先フィールドと要求パス名フィールド（/doc/misc/record.out）に登録された値を、上記処理で得た移送先ファイルサーバ（100.0.0.101）とパス名（/200.0.0.101/doc/misc/record.out）へ変更し、さらに、送元フィールドに自分のアドレス（200.0.0.101）をセットする（図 1 6 の変換後要求パケットを参照）。

【 0 1 0 5 】

そして、ファイルサーバ105Cは、作成した変換後要求パケットを、移送先ファイルサーバ（本例ではファイルサーバ105A）へ送信する。変換後要求パケットを受信した移送先ファイルサーバは、その内容で指定されるファイルを読み出して応答パケット（本例では図 1 7 の変換前応答パケット）を作成し、ファイルサーバ105Cへ返信する（ステップ1906）。

【 0 1 0 6 】

移送先ファイルサーバより応答パケットを受信したファイルサーバ105Cは、その応答パケットの内容を次のように変換する。応答パケットの宛先フィールドの値（200.0.0.101）を、read要求パケットを発行したクライアント103Cのアドレス（200.0.0.1）に、送元フィールドの値をファイルサーバ105Cのアドレス（200.0.0.101）に、応答パス名フィールドの値をクライアント103Cから受信した変換前要求パケットの要求パス名フィールドに登録された値に変換する（図 1 7 の変換後応答パケットを参照）。

【 0 1 0 7 】

変換終了後、ファイルサーバ105Cは、変換して作成した応答パケットを、クライアント103Cへ送信する(ステップ1907)。

【0 1 0 8】

最後に、ファイルサーバ105Cは、クライアント103Cに対して、次回以降の同ファイルへのアクセスはファイルサーバ105Aに対して行うように指示するため、移送通知パケットをクライアント103Cに送信し(ステップ1908)、応答処理を完了する。

【0 1 0 9】

移送通知パケットを受信したクライアント103Cでは、以下の二つの処理のうち、いずれか一つが行われる。クライアント103Cが移送通知パケットを認識できる場合、クライアント103Cは、ファイルサーバ105Cから送信された移送通知パケットを受信し、その内容に従ってノード・パス名変換テーブル115を更新する。この処理の結果、移送ファイルへのアクセスは、クライアント103内で移送先ファイルへのアクセスに変換されるようになるため、以後のクライアント103の移送ファイルへのアクセス要求の発行は移送先ファイルサーバに対して直接行なわれる。

【0 1 1 0】

一方、クライアント103が移送通知パケットを認識することが出来ない場合、クライアント103において移送通知パケットは無視される。したがって、クライアント103からの移送ファイルへのアクセス要求は、引き続き移送元であるファイルサーバ105Cに対して発行される。しかし、ファイルサーバ105Cは、クライアント103からの要求を上記と同様の方法で変換し、移送先ファイルサーバへ代理アクセスを実施するため、クライアント103は従来通りの方法によるファイルアクセスの実行が可能である。

【0 1 1 1】

次に、移送ファイルを移送元ファイルサーバへ返還する方法について説明する。ファイルアクセス要求元となるクライアント103は、時間の経過と共に変化する可能性がある。このため、一旦他のファイルサーバ105へ移送したファイルも、移送元ファイルサーバへ返還した方がアクセス性能が向上する場合がある。

【0 1 1 2】

ファイル移送後も、ファイルサーバ105、特に移送先ファイルサーバはアクセス統計テーブル122にファイルアクセスに関する統計情報を引き続き収集し続ける。

【0 1 1 3】

移送先ファイルサーバは、一定時間毎にアクセス統計テーブル122（本例では図18）を検査し、移送ファイルを返還すべきかどうかを以下の方法により検査する。具体的には、移送ファイルが移送元ファイルサーバが属するネットワークグループから集中してアクセスされているかどうかを検査する。

【0 1 1 4】

図19は、移送ファイルの返還処理のうち、返還対象となる移送ファイル（以下、「返還対象ファイル」）を決定する処理手順を示すフローチャートである。本処理は移送先ファイルサーバが、ファイルシステムプログラム120を実行することで、一定時間間隔毎に実施される。

【0 1 1 5】

本処理の実行を開始した移送先ファイルサーバは、特定の条件に合致するファイルをアクセス統計テーブル122から検索する。本例においては、移送先ファイルサーバは、所定の時間、例えば、本処理の開始から1時間前の間に特定のネットワークグループのみから閾値以上の頻度（本例では10回以上）でアクセスが行われたファイルをアクセス統計テーブル122から抽出する。尚、これらの閾値はファイルシステムプログラムにあらかじめ設定するほか、ユーザにより再設定する。本例においては、本処理を開始した時刻が2002/10/1 9:00:00以降ならば、図18のアクセス統計テーブル122に登録されているファイル"/200.0.0.101/doc/misc/record.out"が上述した条件に適合する（ステップ2302）。

【0 1 1 6】

次に、移送先ファイルサーバは、抽出されたファイルがノード・パス名変換テーブル121（本例では図10に示す内容が登録されているとする）の移送先のパス名フィールドに登録されているかどうかを検査する（ステップ2303）。

【0 1 1 7】

抽出されたファイルがノード・パス名変換テーブル121に登録されていれば、そのファイルは移送ファイルであることがわかる。この場合、移送先ファイルサーバは、抽出されたファイルに対応する距離フィールドに登録された値(=5)と、そのファイルの移送元ファイルサーバと要求元ネットワークフィールドに登録されたネットワーク(ここではLAN2)との間の距離(=同一ネットワーク内なので0)を比較する。本処理により、ファイルに集中的にアクセスするネットワークグループと移送先ファイルサーバが属するネットワークグループとの距離が、ファイルに集中的にアクセスするネットワークグループと移送元ファイルサーバが属するネットワークグループとの間の距離よりも大きいかどうかを判定することができる(ステップ2304)。

【0118】

距離フィールドに登録された値の方が大きい場合、すなわち、移送ファイルに集中的にアクセスするネットワークグループと移送先ファイルサーバが属するネットワークグループとの間の距離が、移送ファイルに集中的にアクセスするネットワークグループと移送元ファイルサーバが属するネットワークグループとの間の距離より大きい場合、移送先ファイルサーバは、検索された移送ファイルを返還対象ファイルとして選定する。これは、移送元ファイルサーバへ移送ファイルを返還した方が、ネットワーク間の距離が小さくなり、システムのアクセス性能が向上するからである。

【0119】

返還対象ファイルを選定すると、移送先ファイルサーバは、続いて、返還要請パケット(図20に返還要請パケットの例を示す)を作成する。移送先ファイルサーバは、返還要請パケット作成の際、ノード・パス名変換テーブル121の各エントリに登録されている値を参照して返還要請パケットの各フィールドに値を登録する。その後、移送先ファイルサーバは、移送元ファイルサーバへ返還要請パケットを送信する(ステップ2305)。

【0120】

尚、上述した処理においてファイルが条件を満たさない場合、移送先ファイルサーバは、返還処理を行わずに処理を終了する。

【0 1 2 1】

図 2 1 は、先に決定された返還対象ファイルの返還処理の手順を示すフローチャートである。

【0 1 2 2】

返還要請パケットを受信した移送元ファイルサーバは、返還要請パケットを送信した移送先ファイルサーバ（以下「返還元サーバ」）に対して、返還要請パケットの返還元パス名フィールドに登録されたファイルのread要求を発行する（ステップ2502）。返還元サーバよりファイルを受信した移送元ファイルサーバは、取得したファイルを、返還要請パケットの返還元パス名で指定されたファイル名で自ディスク装置119に格納する（ステップ2503）。さらに、移送元ファイルサーバは、返還元サーバに対して、返還元パス名フィールドで指定されるファイルの削除要求を発行する（ステップ2504）。その後、移送元ファイルサーバは、該サーバが有するノード・パス名変換テーブル121から、返還を受けたファイルのエントリを削除し（ステップ2505）、ファイルの返還処理を完了する。

【0 1 2 3】

尚、返還処理の完了以後に、クライアント103が移送先ファイルサーバに対してアクセス要求を発行した場合、クライアント103は移送先ファイルサーバよりファイルが存在しない旨のエラー応答を受信する。この場合、クライアント103は、該クライアント103のノード・パス名変換テーブル115からエラー応答を受信したファイルのエントリを削除し、移送元ファイルサーバへ再度アクセス要求パケットを発行する。

【0 1 2 4】

第一の実施形態では、「ファイル」を移送の単位として扱った。次に、第一の実施形態の応用として、複数のファイルを下層に含む「ディレクトリ」を移送の単位として扱う第二の実施形態について説明する。

【0 1 2 5】

ファイルシステムにおいては、ディレクトリの配下には、複数のファイルが配されている。第二の実施形態においては、移送したいディレクトリを移送ディレクトリとして指定することにより、同ディレクトリに含まれる全てのファイルの

移送を行うことが出来る。

【0126】

尚、以下に説明するアクセス統計テーブル122の検査手順以外の処理手順は、第一の実施形態と同じ手順であるので、説明を省略する。以下、第二の実施形態におけるアクセス統計テーブル122の検査手順を説明する。

【0127】

図22は、第二の実施形態において、ファイルサーバ105がアクセス統計テーブル122の内容を検査する手順を示すフローチャートである。本処理は、ファイルサーバ105がファイルシステムプログラム120を実行することで、一定時間毎に実行される。

【0128】

ファイルサーバ105は、一定時間毎にアクセス統計テーブル122を検査し、ディレクトリ下のファイルへのアクセスが特定のネットワークグループから集中しておこなわれているかどうかを検査する。もしそのようなディレクトリが見つかったときは、そのディレクトリを移送ディレクトリの候補として選定する。

【0129】

ファイルサーバ105は、まず、アクセス統計テーブル122（図23に示したテーブルであるとする）の中から、ファイルサーバ105が属するネットワークグループとアクセスするネットワークグループとの間の距離が2以上、アクセス回数が10回以上、かつアクセス開始時刻から現在時刻まで一定時間（例として1時間）以上経過している（その間、他のネットワークグループからのアクセスはない）ファイルを検索する。本ステップにより発見されるファイルを(d)とする。本例では、"/doc/misc/record.out"が該当する(ステップ2602)。尚、検索の条件は本例に限られない。ただしこれらの閾値はファイルシステムプログラムにあらかじめ設定するほか、ユーザにより再設定する。

【0130】

アクセス統計テーブル122に(d)が存在した場合、ファイルサーバ105は、当該ファイルを含むディレクトリ（図23の例では"/doc/misc/"）を認識し(d1)とする。また、当該ファイルに対応する要求元ネットワークフィールドに登録された

ネットワークを認識し(N) (図 2 3 の例では、"100.0.0.0/24") とする(ステップ 2603)。

【 0 1 3 1 】

次に、ファイルサーバ105は、アクセス統計テーブル122の全エントリの中から、ファイルが(d1)の配下でかつ要求元ネットワークフィールドに登録されているネットワークが(N)以外のエントリを検索する。これを(e)とする (図 2 3 では該当するファイルはない) (ステップ2605)。

【 0 1 3 2 】

(e)が存在する場合、(d1)には異なるネットワークグループからアクセスされるファイルが混在していることになる。このため、(d1)配下のファイルを全て移送することはシステムの性能低下を招く。したがって、ファイルサーバ105はディレクトリである(d1)の移送をあきらめ、(d)を移送ファイルの候補として選択する(ステップ2608)。

【 0 1 3 3 】

(e)が存在しない場合、(d1)配下のファイルはネットワーク(N)以外のネットワークグループからアクセスを受けていないため、ファイルサーバ105は、(d1)を移送ディレクトリの候補として選択することができる。

【 0 1 3 4 】

しかし、(d1)よりも1階層上位のディレクトリ (図 2 3 の例では"/doc/") を移送ディレクトリの候補として選択できる可能性もある。このため、ファイルサーバ105は、次に、(d1)を新たな(d)、(d1)の上位階層のディレクトリを新たな(d1)として(ステップ2607)、ステップ2604以降の処理を再度実施する。すなわち、アクセス統計テーブル122の全エントリの中から、新たな(d1)配下のファイルで、要求元ネットワークフィールドに登録されているネットワークが(N)以外のエントリを検索する。検索の結果得られるファイルのエントリを(e)とする (図 2 3 では"doc/memo.txt"が該当する)。

【 0 1 3 5 】

ファイルサーバ105は、上記処理を繰り返し、エントリ(e)が見つかった時点で処理の繰り返しを中止する。そして、中止時までには選択された移送ディレクトリ

の候補（またはファイル）(d)を移送ディレクトリの候補とし(ステップ2608)、処理を終了する。

【0136】

尚、ディレクトリ単位で移送する第二の実施形態においても、第一の実施形態の図14に示すように、移送先ファイルサーバがクライアント103からのアクセス要求を受けてからファイルの実体を移送するため、必要なデータのみがその都度ネットワーク101上で転送される。つまり、移送ディレクトリに含まれる移送ファイル全てを同時に移送しない。このため、ネットワーク101のトラフィックを分散させ、また、ファイルサーバ105の負荷を分散させる効果がある。

【0137】

次の第三の実施形態について説明する。第一の実施形態では、移送元ファイルサーバは、ファイルに集中的にアクセスするネットワークグループに含まれるファイルサーバ105の中から、移送先サーバを選択した。このため、ファイルに集中的にアクセスするネットワークグループに含まれるファイルサーバ105の中に条件（空き容量が指定量以上かつ、管理者が移送元サーバと同一、など）が適合するファイルサーバ105が存在しない場合、第一の実施形態においては、移送元ファイルサーバは移送を行わないこととした。

【0138】

しかし、以下に示す第三の実施形態では、ファイルに集中的にアクセスするネットワークグループに含まれるファイルサーバ105に、条件に適合するファイルサーバ105が見つからなかった場合に、他のネットワークグループに条件に適合するファイルサーバ105が存在すれば、移送元ファイルサーバは、次善の策としてそのファイルサーバ105へファイルの移送をおこなう。

【0139】

図23は、第三の実施形態のシステム構成を示す図である。本実施形態のシステムは、2つのネットワークLAN1、LAN3がインターネットやWANを介して接続され、LAN2はインターネット104を介してLAN3と接続されている。LAN2とLAN1とはLAN3を経由してのみ接続されている。

【0140】

第三の実施形態での処理は、以下に説明する移送先ファイルサーバの選択手順を除き、第一の実施形態での処理手続きと同じであるので、それらの処理については説明を省略する。以下に、第三の実施形態の移送先ファイルサーバの選択方法を説明する。

【0141】

図25は、第三の実施形態における、ファイルサーバ105における移送先ファイルサーバ選択処理の手順を示すフローチャートである。本処理は、移送元ファイルサーバが移送ファイルの候補を選定したときに実行される。以下、図24において、移送元ファイルサーバがファイルサーバ105Cである場合で説明する。

【0142】

移送ファイルの候補を選定した移送元ファイルサーバは、アクセス統計テーブル122から、移送ファイルの候補へアクセスを行うネットワークグループに対応するネットワーク（100.0.0.0/24：LAN1）へ移送先検索パケットをブロードキャストする（ステップ3002）。

【0143】

移送元ファイルサーバは、返送された移送許可パケットの内容を確認し、予め指定された条件を満たすかどうか判定する。本例においては、LAN1に接続されたファイルサーバ105A及び105Bから移送許可パケットが返送され、移送元ファイルサーバは、これらの移送許可パケットが条件（空き容量が指定量以上かつ、管理者が移送元サーバと同一、など）に適合するかどうかを検査する（ステップ3003）。

【0144】

いずれの移送許可パケットも条件に適合しない場合、移送元ファイルサーバは、移送先検索パケットをブロードキャストするネットワークの対象を拡大する。具体的には、移送元ファイルサーバは、先に移送先検索パケットをブロードキャストしたネットワーク（LAN1）について、ネットワークマスクビットを短縮（例では、マスクビットを24bit(255.255.255.0)から16bit(255.255.0.0)に短縮）し、LAN1と同じ上位16ビットのアドレスを有するLAN3（100.0.1.0/24）に移送先検索パケットをブロードキャストする（ステップ3004、3005）。

【0145】

その結果、ネットワークLAN3に属するファイルサーバ105D (100.0.1.102) から移送許可パケットが移送元ファイルサーバに返送される。その後、移送元ファイルサーバは、ファイルサーバ105Dからの移送許可パケットが条件に適合するかどうか検査する(ステップ3006)。ファイルサーバ105Dからの移送許可パケットが条件と適合している場合、移送元ファイルサーバは、ファイルサーバ105Dを移送先ファイルサーバとして選択する(ステップ3007)。条件に適合するファイルサーバ105が無ければ、移送元ファイルサーバは、移送先ファイルサーバ無し判断して、ファイルの移送は行わない(ステップ3008)。

【0146】

第三の実施形態によれば、移送元ファイルサーバは、アクセスを集中して行うネットワークグループに移送先ファイルサーバが見つからない場合にも、次善の策として、アクセスを集中して行うネットワークグループとは別のネットワークグループに属するファイルサーバ105へファイルを移送することができる。

【0147】**【発明の効果】**

本発明によれば、クライアントから遠隔地にあるファイルサーバが管理するファイルへのアクセス性能を向上させることができる。また、キャッシュ方式に比べ一貫性制御が不要なため、ネットワークに余分なトラフィックを発生させることも無い。

【図面の簡単な説明】

【図1】 システムの概要を示す図。

【図2】 アクセス要求パケットの例を示す図。

【図3】 アクセス統計テーブルの例を示す図。

【図4】 アクセス統計テーブルの更新処理の手順を示すフローチャート。

【図5】 移送ファイルの候補を決定する処理手順の例を示すフローチャート。

【図6】 移送先検索パケットの例を示す図。

【図7】 移送受け入れ判定処理の手順の例を示すフローチャート。

【図8】 移送許可パケットの例を示す図。

【図 9】 移送先ファイルサーバの選択手順の例を示すフローチャート。

【図 1 0】 ノード・パス名変換テーブルの例を示す図。

【図 1 1】 移送通知パケットの例を示す図。

【図 1 2】 アクセス変換処理の手順を示すフローチャート。

【図 1 3】 変換前／変換後のアクセス要求パケットの例を示す図。

【図 1 4】 移送先ファイルサーバの処理手順の例を示すフローチャート。

【図 1 5】 移送元ファイルサーバの処理手順の例を示すフローチャート。

【図 1 6】 移送元ファイルサーバによる要求パケットの変換例を示す図。

【図 1 7】 移送元ファイルサーバによる応答パケットの変換例を示す図。

【図 1 8】 アクセス統計テーブルの例を示す図。

【図 1 9】 返還するファイルを決定する処理手順を示すフローチャート。

【図 2 0】 返還要請パケットの例を示す図。

【図 2 1】 ファイルの返還処理の手順の例を示すフローチャート。

【図 2 2】 移送対象の候補となるディレクトリを決定する処理手順の例を示す図。

【図 2 3】 アクセス統計テーブルの例を示す図。

【図 2 4】 第三の実施形態のシステムの全体を示す図。

【図 2 5】 移送先サーバの選択処理の手順を示すフローチャート。

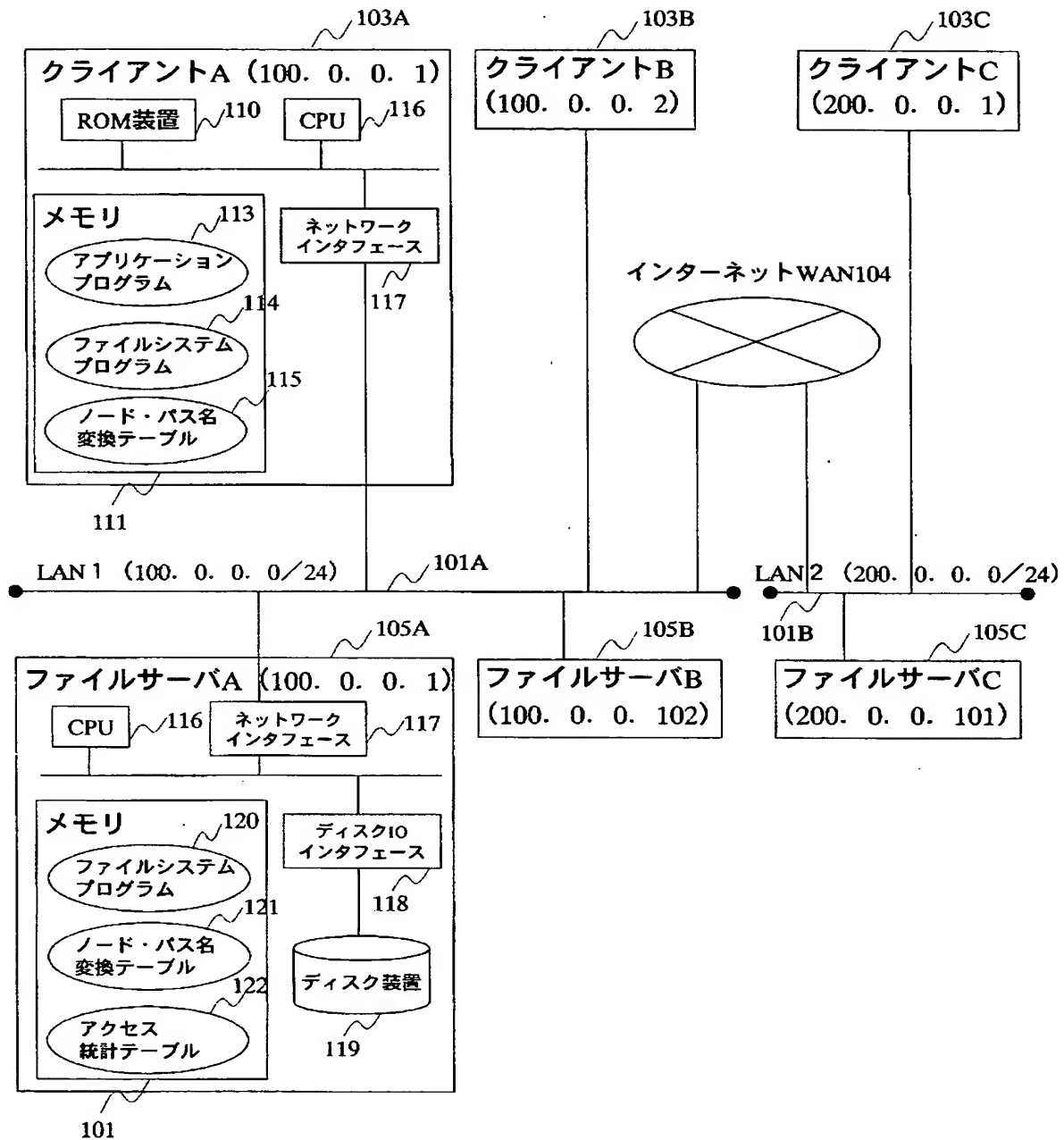
【符号の説明】

1 0 1…LAN、1 0 3…クライアント、1 0 5…ファイルサーバ、1 0 9…CPU、1 1 0…ROM装置、1 1 1…メモリ、1 1 2…ネットワークインターフェイス、1 1 9…ディスク装置。

【書類名】 図面

【図 1】

図 1



【図 2】

図 2

A

宛先(サーバ)	200.0.0.101
送り元(クライアント)	100.0.0.1
要求種別	read
要求パス名	/doc/misc/sample.log
オフセット[byte]	4096
サイズ[byte]	1024

B

宛先(サーバ)	200.0.0.101
送り元(クライアント)	100.0.0.1
要求種別	write
要求パス名	/doc/misc/sample.log
オフセット[byte]	4096
サイズ[byte]	1024
データ	データ本体

C

宛先(サーバ)	100.0.0.1
送り元(クライアント)	200.0.0.101
要求種別	read
要求パス名	/doc/misc/sample.log
オフセット[byte]	4096
サイズ[byte]	1024
データ	データ本体

D

宛先(サーバ)	100.0.0.1
送り元(クライアント)	200.0.0.101
要求種別	write
要求パス名	/doc/misc/sample.log
オフセット[byte]	4096
サイズ[byte]	1024

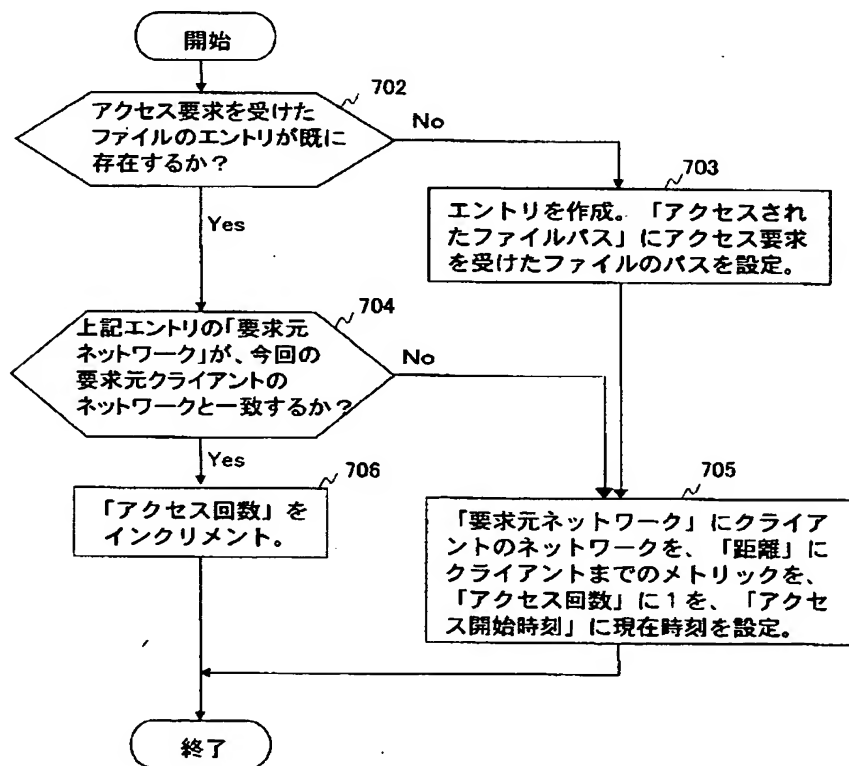
【図 3】

図 3

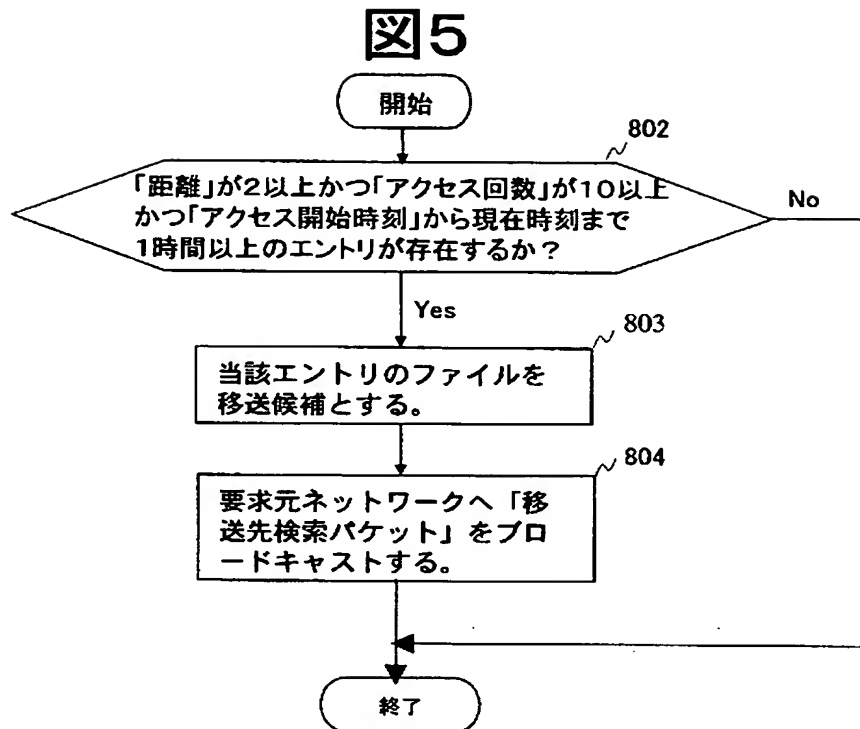
アクセスされた ファイルパス (601)	要求元 ネットワーク (602)	距離 (603)	アクセス回数 (604)	アクセス開始 時刻 (605)
/doc/misc/record.out	100.0.0.0/24	5	120	2002/9/1 10:00:00
/doc/misc/sample.log	100.0.0.0/24	5	85	2002/9/2 11:00:00
/doc/memo.txt	200.0.0.0/24	1	45	2002/9/2 11:00:05

【図 4】

図 4



【図 5】

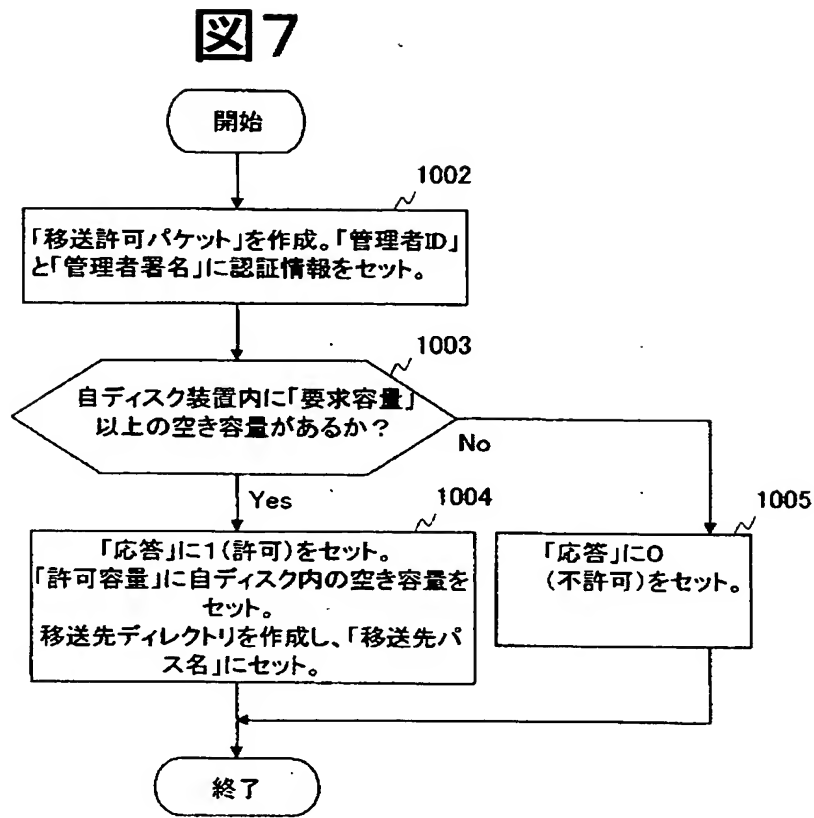


【図 6】

図 6

宛先ネットワーク(IPヘッダ内)	100.0.0.0/24
送り元サーバ(IPヘッダ内)	200.0.0.101
移送ID	0x100
移送元サーバ	200.0.0.101
要求容量[MB]	100

【図 7】

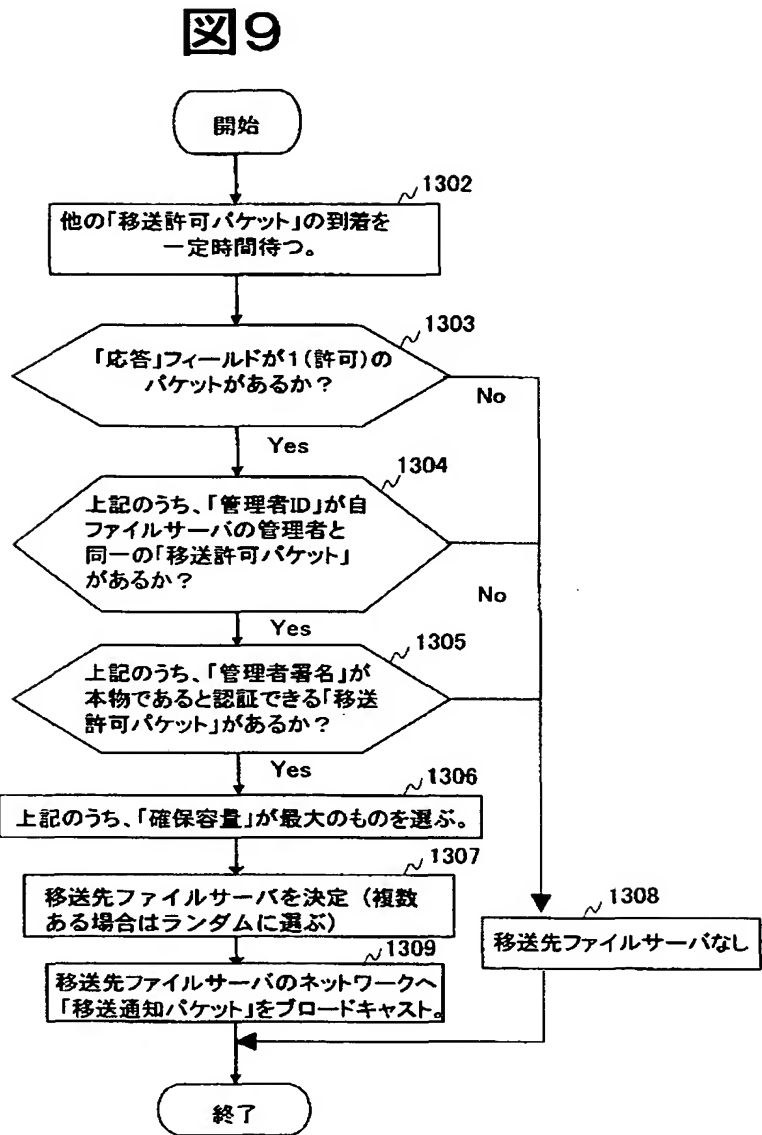


【図 8】

図 8

A		B	
宛先サーバ	200.0.0.101	宛先サーバ	200.0.0.101
送り元サーバ	100.0.0.101	送り元サーバ	100.0.0.102
移送ID	0x100	移送ID	0x100
応答	1	応答	1
移送先サーバ	100.0.0.101	移送先サーバ	100.0.0.102
移送先パス名	/200.0.0.101/	移送先パス名	/200.0.0.101/
確保容量[MB]	256	確保容量[MB]	128
管理者ID	foo	管理者ID	foo
管理者署名	oekdigke	管理者署名	oekdigke

【図 9】



【図 10】

図10

移送ID (1401)	移送元		移送先	
	ノード (1402)	パス名 (1403)	ノード (1404)	パス名 (1405)
0x100	200.0.0.101	/doc/misc/record.out	100.0.0.101	/200.0.0.101/doc/misc/record.out

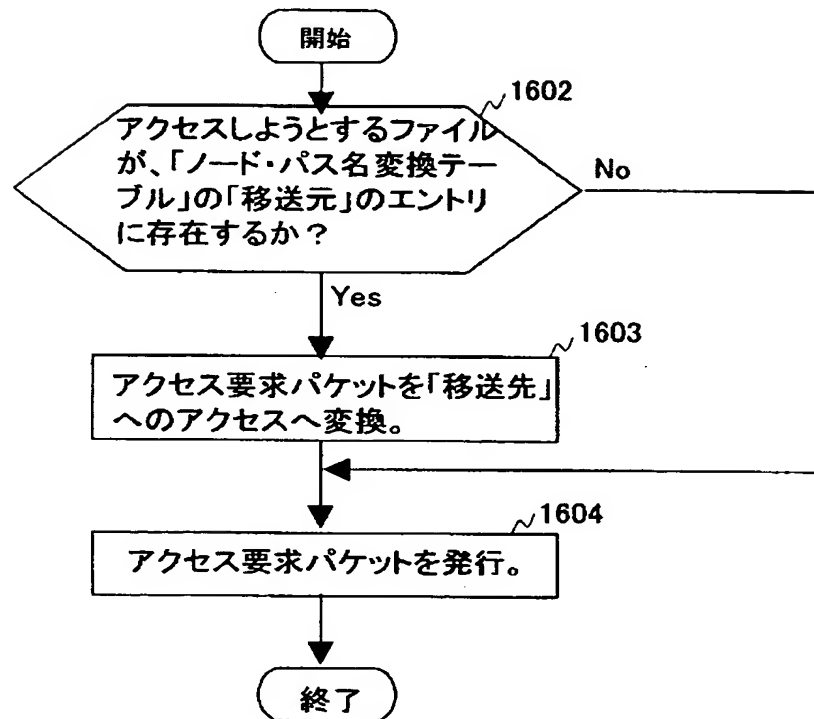
【図 11】

図 11

宛先サーバ	100.0.0.0/24
送り元サーバ	200.0.0.101
移送ID	0x100
移送元サーバ	200.0.0.101
移送元パス名	/doc/misc/record.out
移送先サーバ	100.0.0.101
移送先パス名	/200.0.0.101/doc/misc/record.out

【図 12】

図 12



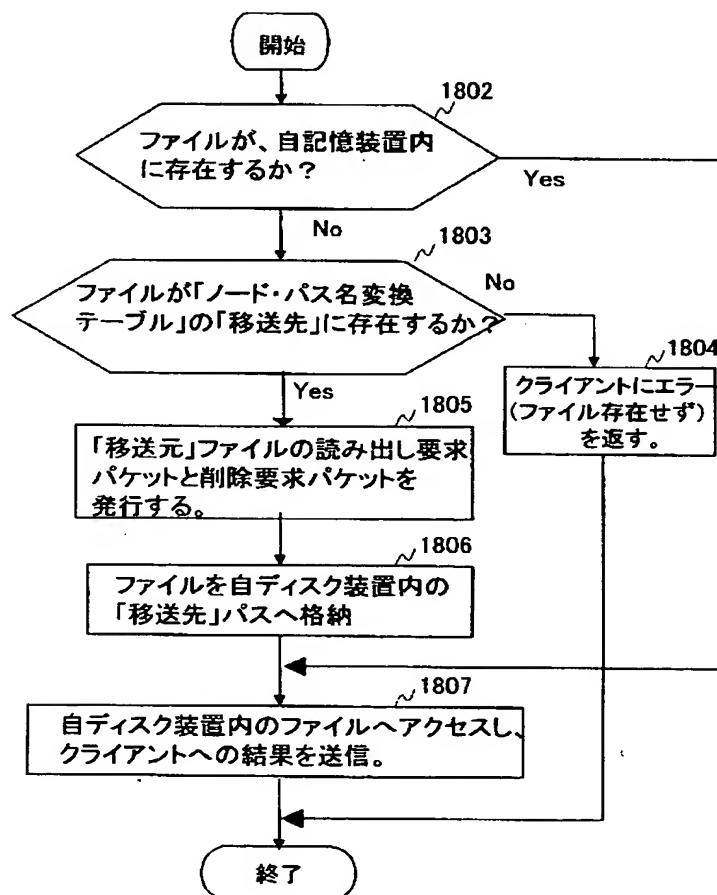
【図 13】

図13

変換前		変換後	
宛先(サーバ)	200.0.0.101	宛先(サーバ)	100.0.0.101
送り元(クライアント)	100.0.0.1	送り元(クライアント)	100.0.0.1
要求種別	read	要求種別	read
要求パス名	/doc/misc/record.out	要求パス名	/200.0.0.101/doc/misc/record.out
オフセット[byte]	4096	オフセット[byte]	4096
サイズ[byte]	1024	サイズ[byte]	1024

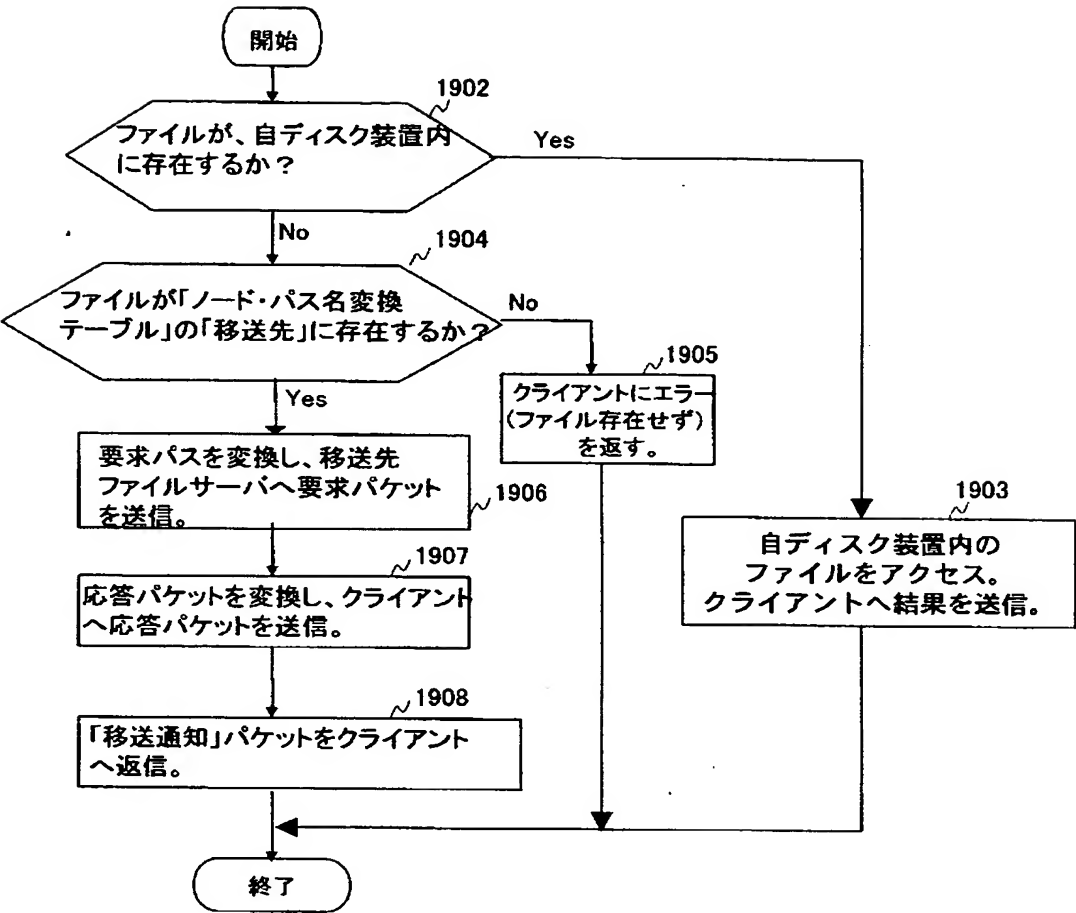
【図 14】

図14



【図 15】

図15



【図 16】

図16

変換前要求パケット		変換後要求パケット	
宛先	200.0.0.101	宛先	100.0.0.101
送り元	200.0.0.1	送り元	200.0.0.101
要求種別	read	要求種別	read
要求パス名	/doc/misc/record.out	要求パス名	/200.0.0.101/doc/misc/record.out
オフセット[byte]	4096	オフセット[byte]	4096
サイズ[byte]	1024	サイズ[byte]	1024

【図 17】

図 17

変換前応答パケット		変換後応答パケット	
宛先	200.0.0.101	宛先	200.0.0.1
送り元	100.0.0.101	送り元	200.0.0.101
要求種別	read	要求種別	read
要求パス名	/200.0.0.101/doc/misc/record.out	要求パス名	/doc/misc/record.out
オフセット[byte]	4096	オフセット[byte]	4096
サイズ[byte]	1024	サイズ[byte]	1024
データ	データ本体	データ	データ本体

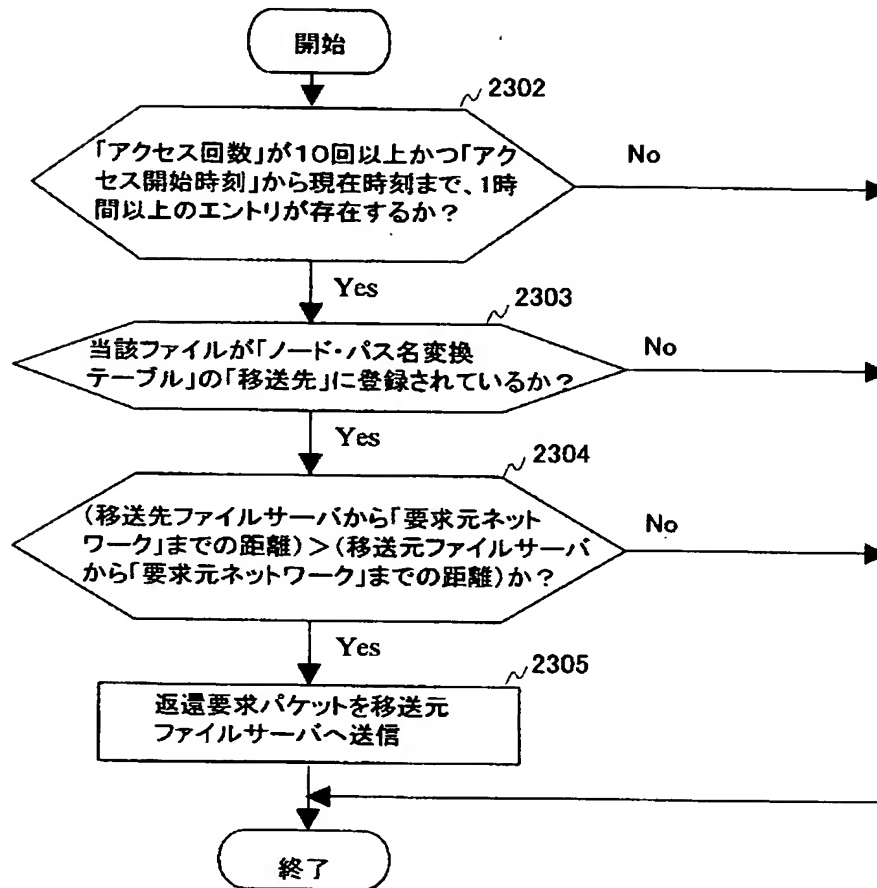
【図 18】

図 18

アクセスされた ファイルパス	要求元 ネットワーク	距離	アクセス回数	アクセス開始 時刻
/200.0.0.101/doc/misc/record.out	100.0.0.0/24	5	200	2002/10/1 18:00:00

【図 19】

図 19



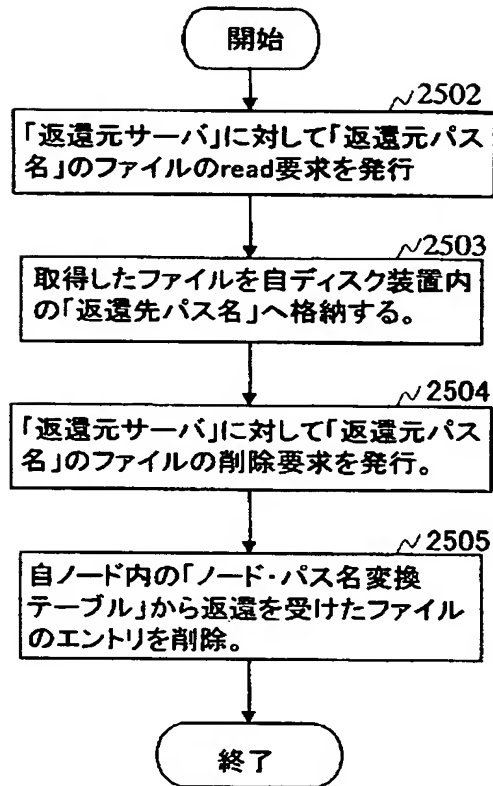
【図 20】

図 20

宛先サーバ	200.0.0.101
送り元サーバ	100.0.0.101
移送ID	0x100
返還元サーバ	100.0.0.101
返還元パス名	/200.0.0.101/doc/misc/record.out
返還先サーバ	200.0.0.101
返還先パス名	/doc/misc/record.out

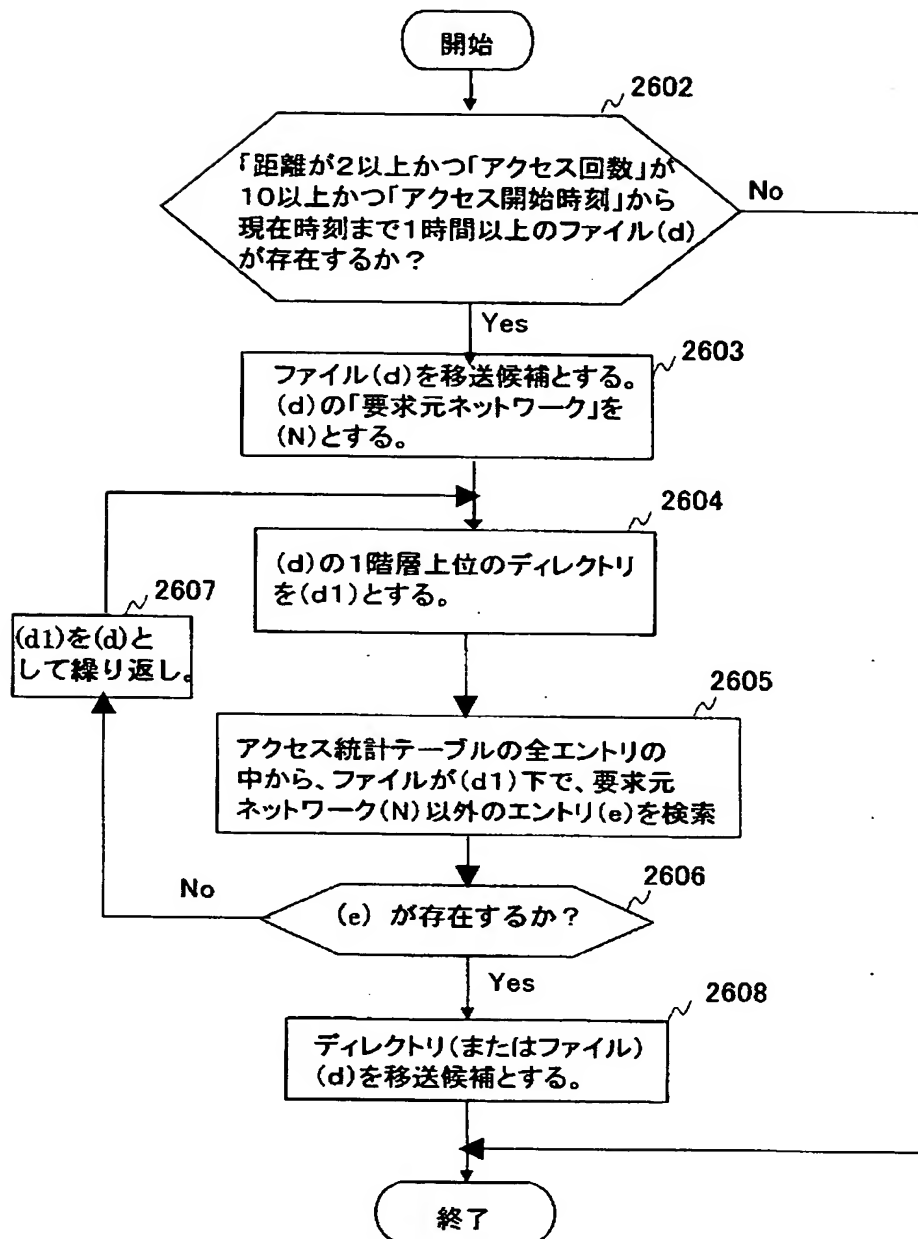
【図 21】

図 21



【図 22】

図22



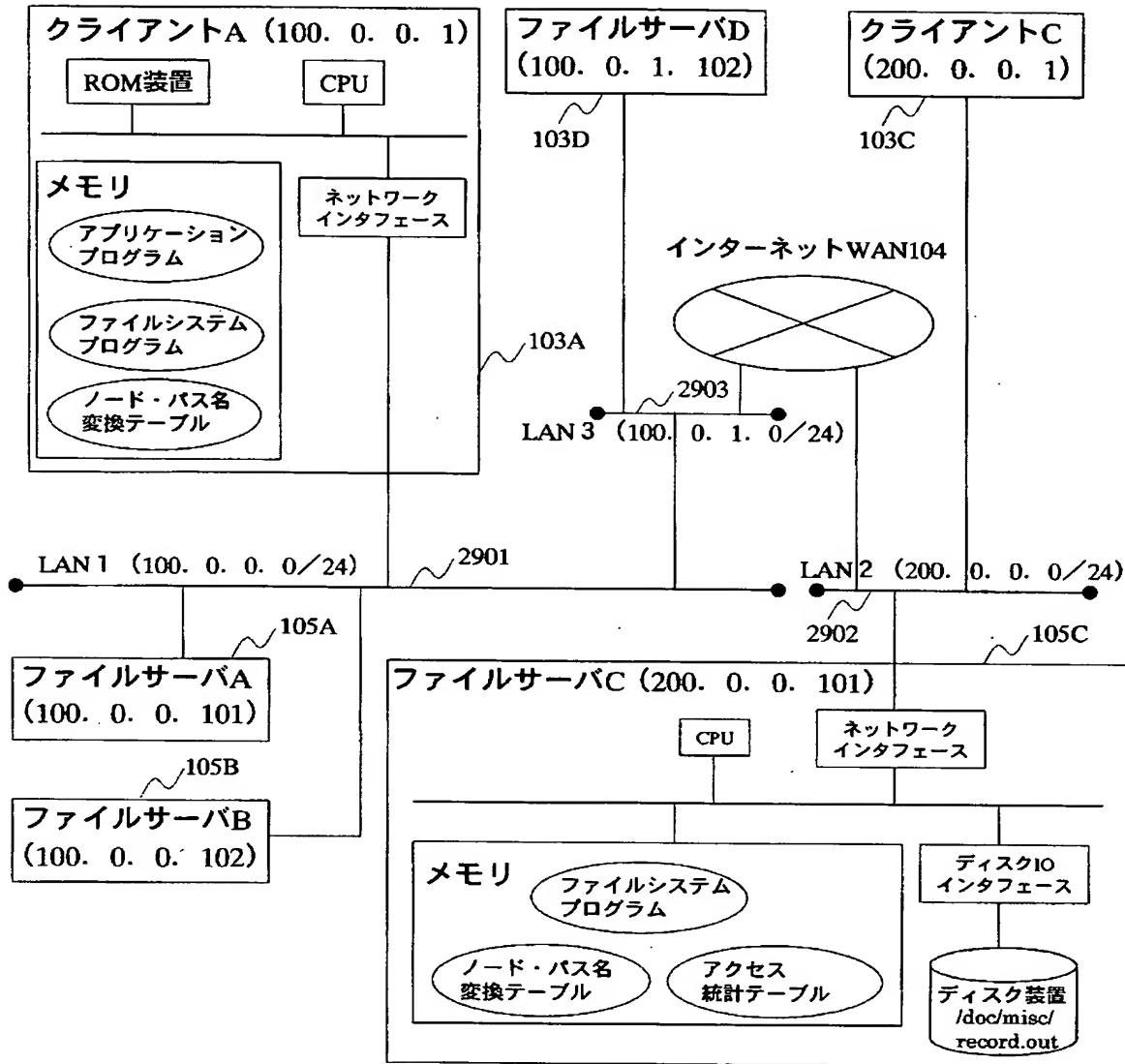
【図 2 3】

図 23

アクセスされた ファイルパス	要求元 ネットワーク	距離	アクセス回数	アクセス開始 時刻
/doc/misc/record.out	100.0.0.0/24	5	120	2002/9/1 10:00:00
/doc/misc/sample.log	100.0.0.0/24	5	105	2002/9/2 10:00:04
/doc/memo.txt	200.0.0.0/24	1	45	2002/9/2 10:00:30
/doc/misc/work/tmp.txt	100.0.0.0/24	5	40	2002/9/1 10:00:04

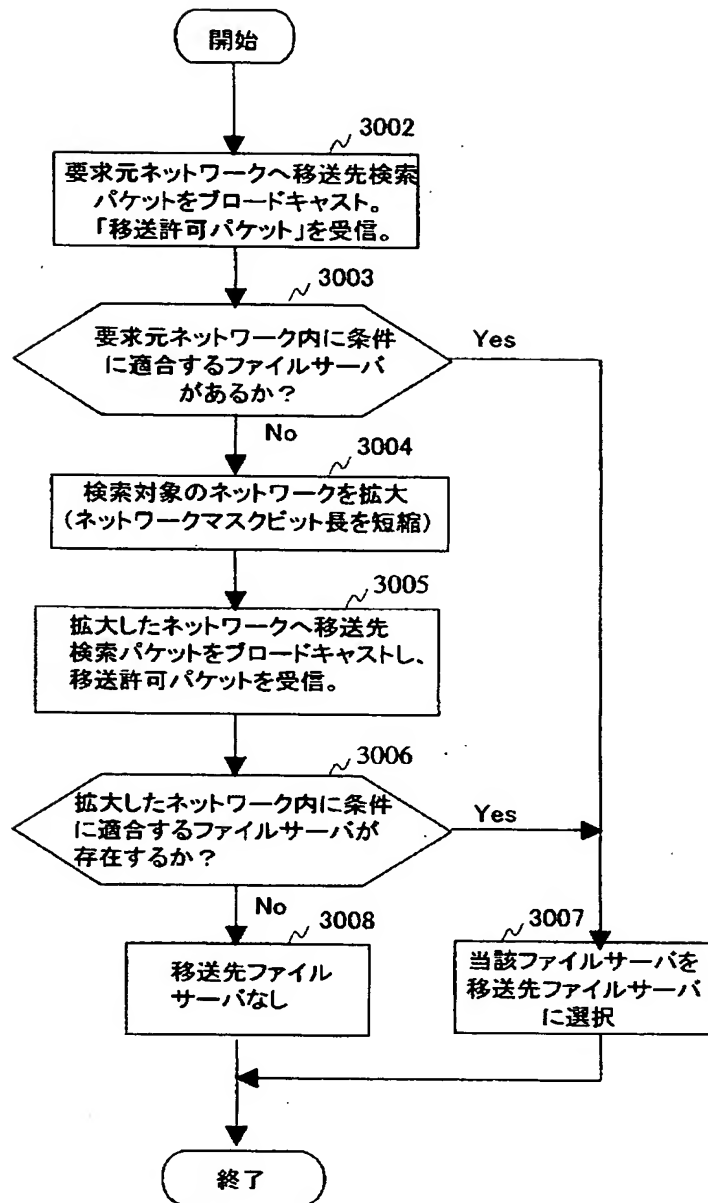
【図 24】

図24



【図 25】

図25



【書類名】 要約書**【要約】****【課題】**

クライアントおよびファイルサーバがネットワークにより接続され、クライアントがネットワークを介してファイルサーバに接続されたディスク記憶装置内のファイルをアクセスするシステムにおいて、クライアントから遠隔地のファイルサーバ内のファイルへのアクセス性能が低下する。

【解決手段】

ファイルサーバがクライアント付近のファイルサーバを検索し、発見したファイルサーバへファイルを移送する。クライアントは移送先ファイルサーバへ当該ファイルをアクセスする。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 1 1 5 1 8 3
受付番号	5 0 3 0 0 6 5 1 9 1 7
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 5 年 4 月 2 2 日

< 認定情報・付加情報 >

【提出日】 平成15年 4月21日

次頁無

特願 2003-115183

出願人履歴情報

識別番号

[000005108]

1. 変更年月日

1990年 8月31日

[変更理由]

新規登録

住 所

東京都千代田区神田駿河台4丁目6番地

氏 名

株式会社日立製作所